St Chad's Catholic & Church of England High School

E-Safety Policy

Updated November 2016

Our e–Safety Policy has been written by the school taking current comprehensive advice and government guidance (it reflects the Prevent Duty guidance and Keeping Children Safe in Education 2016 information). Our School Policy has been agreed by the Senior Leadership Team and approved by governors. The e–Safety Policy and its implementation will be reviewed annually.

Use of the Internet

The Internet use is part of the statutory curriculum and is seen as a necessary tool for learning. It is a part of the everyday life for education, business and social interaction within the school. We recognise that as such we have a duty to provide students with quality Internet access as part of their learning experience. Internet usage in school is carried out in conjunction with the schools Internet Policy. 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. The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. Internet access is an entitlement for students who show a responsible and mature approach to its use.

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 school uses a filtering system and physical monitoring of Internet usage to ensure students are safe and not exposed to inappropriate web content. The school will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law. Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils. Staff

should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability. 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 to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

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. The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum. The security of the school information systems and users will be reviewed regularly. Virus protection will be updated regularly. Personal data sent over the Internet or taken off site will be encrypted. Portable media may not used without specific permission followed by an anti-virus/malware scan. Unapproved software will not be allowed in work areas or attached to email. Files held on the school's network will be regularly checked. The ICT coordinator/network manager will review system capacity regularly. The use of user logins and passwords to access the school network will be enforced.

Email

Pupils may only use approved email accounts for school purposes.

- **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.**
- **Whole -class or group email addresses will be used in primary schools for communication outside of the school.**
- **Staff will only use official school provided email accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Team. The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.**
- **Email addresses will be published carefully online, to avoid being harvested for spam (e.g. by replacing '@' with 'AT'.)**
- **The head teacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.**
- **The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.**

Images/Video

Images or videos that include pupils will be selected carefully and will not provide material that could be reused.

- **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.**
- **Pupils work can only be published with their permission or the parents.**
- **Written consent will be kept by the school where pupils' images are used for publicity purposes, until the image is no longer in use.**
- **The School will have a policy regarding the use of photographic images of children which outlines policies and procedures.**

The school will control access to social media and social networking sites.

- **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 etc.**
- **Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the Senior Leadership Team before using Social Media tools in the classroom.**
- **Staff official blogs or wikis should be password protected and run from the school website with approval from the Senior Leadership Team. Members of staff are advised not to run social network spaces for pupil use on a personal basis.**
- **Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.**

The school's broadband access will include filtering appropriate to the age and maturity of pupils.

- **The school will work with the local authority 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. All members of the school community (all staff and all pupils) will be aware of this procedure.**
- **If staff or pupils discover unsuitable sites, the URL will be reported to the School e-Safety Coordinator who will then record the incident and escalate the concern as appropriate.**
- **The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.**
- **Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team.**
- **The School Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective.**

• Any material that the school believes is illegal will be reported to appropriate agencies such as Police or CEOP.
• The school's access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from network managers.
Video Conferencing
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 should 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.
• The equipment must be secure and if necessary locked away when not in use.
• School videoconferencing equipment will not be taken off school premises without permission.
• Responsibility for the use of the videoconferencing equipment outside school time will be established with care.
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.**

• Only key administrators should be given access to videoconferencing administration areas or remote control pages.
• Unique log on and password details for the educational videoconferencing services should only be issued to members of staff and kept secure.
Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
• Pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school Acceptable Use or Mobile Phone Policy.

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.

- **All staff will read and sign the 'Staff Information Systems Code of Conduct' or School Acceptable Use Policy before using any school ICT resources.**

• Parents will be asked to read the School Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.
• All visitor 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.
• When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).
All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc).
• The e-Safety Coordinator 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.
• After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
• Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children's Safeguard Team or e-Safety officer and escalate the concern to the Police.
• If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Area Children's Officer or the County e-Safety Officer.
• If an incident of concern needs to be passed beyond the school then the concern will be escalated to the e-Safety officer to communicate to other school in Kent.
Complaints about Internet misuse will be dealt with under the School's complaints procedure.
• Any complaint about staff misuse will be referred to the head teacher.
• All e–Safety complaints and incidents will be recorded by the school, including any actions taken.
• Pupils and parents will be informed of the complaints procedure.
• Parents and pupils will need to work in partnership with the school to resolve issues.
• All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
• Discussions will be held with the local Police Safer Schools Partnership Coordinators and/or Children's Safeguard Team to establish procedures for handling potentially illegal issues.
• Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.
• All members of the school community will be reminded about safe and appropriate

behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.

- **There are clear procedures in place to support anyone in the school community affected by cyberbullying.**
- **All incidents of cyberbullying reported to the school will be recorded.**
- **There will be clear procedures in place to investigate incidents or allegations of Cyberbullying.**

SLT and staff will regularly monitor the usage of the LP by pupils and staff in all areas, in particular message and communication tools and publishing facilities.

- **Pupils/staff will be advised about acceptable conduct and use when using the LP.**
- **Only members of the current pupil, parent/carers and staff community will have access to the LP.**
- **All users will be mindful of copyright issues and will only upload appropriate content onto the LP.**
- **When staff, pupils etc leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.**

• Any concerns about content on the LP may be recorded and dealt with in the following ways:

• A visitor may be invited onto the LP by a member of the SLT. In this instance there may be an agreed focus or a limited time slot.

• Pupils may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.

a) The user will be asked to remove any material deemed to be inappropriate or offensive.

b) The material will be removed by the site administrator if the user does not comply.

c) Access to the LP for the user may be suspended.

d) The user will need to discuss the issues with a member of SLT before reinstatement.

e) A pupil's parent/carer may be informed.

The use of mobile phones and other personal devices by students and staff in school will be decided by the school and covered in the school Acceptable Use or Mobile Phone Policies.

- **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.**
- **School staff may confiscate a phone or device if they believe it is being used to contravene the schools behaviour or bullying policy. The phone or device might be searched by the Senior Leadership team with the consent of the**

pupil or parent/carer. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.

• Mobile phones and personal devices will not be used during lessons or formal school time. They should be switched off at all times.

All users will be informed that network and Internet use will be monitored.

• An e–Safety training programme will be established across the school to raise the awareness and importance of safe and responsible internet use amongst pupils.

• Pupil instruction regarding responsible and safe use will precede Internet access.

• An e–Safety module will be included in the PSHE, Citizenship and/or ICT programmes covering both safe school and home use.

• e–Safety training will be part of the transition programme across the Key Stages and when moving between establishments.

• e-Safety rules or copies of the student Acceptable Use Policy will be posted in all rooms with Internet access.

• Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.

• Particular attention to e-Safety education will be given where pupils are considered to be vulnerable.

E-Safety Co-ordinator

The School e-Safety Coordinator is
……

Policy approved by Head Teacher: ……

Date: ……

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

Date: ……Date for the next policy review is……