Holy Cross Boys' Primary School
E-SAFETY POLICY

The need for an e-safety Policy

National guidance suggests that it is essential for schools to take a leading role in e-safety. Becta in its "Safeguarding Children in a Digital World" suggested:

> "That schools support parents in understanding the issues and risks associated with children's use of digital technologies. Furthermore, Becta recommends that all schools have acceptable use policies, and ensure that parents are aware of the procedures for e-safety within the school. Recognising the growing trend for home-school links and extended school activities, Becta recommends that schools take an active role in providing information and guidance for parents on promoting e-safety messages in home use of ICT, too."

The Byron Review "Safer Children in a Digital World" stressed the role of schools:

> "One of the strongest messages I have received during my Review was about the role that schools and other services for children and families have to play in equipping children and their parents to stay safe online. To empower children and raise the skills of parents, I make recommendations to Government in the following areas: delivering e-safety through the curriculum, providing teachers and the wider children's workforce with the skills and knowledge they need, reaching children and families through Extended Schools and taking steps to ensure that Ofsted holds the system to account on the quality of delivery in this area."

The development and expansion of the use of ICT, and particularly of the internet, has transformed learning in schools in recent years. Children and young people will need to develop high level ICT skills, not only to maximise their potential use as a learning tool, but also to prepare themselves as lifelong learners and for future employment. There is a large body of evidence that recognises the benefits that ICT can bring to teaching and learning. Schools have made a significant investment both financially and physically to ensure these technologies are available to all learners. The benefits are perceived to "outweigh the risks." However, schools must, through their e-safety policy, ensure that they meet their statutory obligations to ensure that children and young people are safe and are protected from potential harm, both within and outside school. This policy will also form part of the school's protection from legal challenge, relating to the use of ICT.

1.1 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 and for child protection.
• The school will appoint an e-Safety Coordinator. This may be the Designated Child Protection Coordinator as the roles overlap.
• Our e-Safety Policy has been written, building on the Warwickshire ICT Development Service e-Safety Policy and government guidance. It has been agreed by the senior management and approved by governors.
• The e-Safety Policy will be reviewed annually.

1.2 Teaching and learning
1.2.a Why Internet use is 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.

1.2.b Internet use will enhance learning
• The school Internet access is expressly for pupil and Teacher use and includes filtering appropriate to the age of pupils.
• Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
• Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
• Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.

1.2.c Pupils will be taught how to evaluate Internet content
• If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to the school e-safety officer and in turn C2k.
• Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
• Lessons will be given in e-safety and sensible use of the internet.

1.3 Managing Internet Access
1.3.a Information system security
• The security of the school information systems will be reviewed regularly.
• Virus protection will be installed and updated regularly.
• The school uses the C2k Broadband with its firewall and filters.

1.3.b 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.
• Whole-class or group e-mail addresses could be used in KS1 primary classes.

1.3.c Published content and the school web site
• The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
• The ICT coordinator will take overall editorial responsibility and ensure that content is accurate and appropriate.

1.3.d Publishing pupil's images and work
• Photographs that include pupils will be selected carefully and will only contain those pupils whose parents have signed a photographic consent form (Appendix 1).
• Pupils' full names will not be used anywhere on the Web site, particularly in association with photographs.
• Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.

1.3.e Social networking and personal publishing
• Social networking sites and newsgroups will be blocked unless a specific use is approved.
• Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc.

1.3.f Managing filtering
• The school will work in partnership with C2k to ensure filtering systems are as effective as possible.
• If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the school E-Safety coordinator.

1.3.g Managing videoconferencing (for the future)
• Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
• Videoconferencing should be supervised appropriately for the pupils' age.
• The only time videoconferencing should take place is when the ICT coordinator has arranged a conference through the Learning NI portal and only for educational purposes.

1.3.h 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.

1.3.i Protecting personal data
• Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

1.4 Policy Decisions
1.4.a Authorising Internet access
• The school will maintain a current record of all staff and pupils who are granted Internet access.
• All students will have the Acceptable use Policy read and explained to them by their teacher every year and they must sign the Acceptable ICT use agreement, 'Student/Pupil Acceptable Use Agreement Form'. (Appendix 1)
• All staff must read and sign the acceptable ICT use agreement, 'Staff and Volunteer Acceptable Use Policy Agreement', before using any school ICT resource. (Appendix 2)
•All Parents of KS2 children must read and sign the document, 'Parent/Carer Acceptable Use Policy Agreement' before their son can be granted access to the use of any ICT equipment within the school. (Appendix 3)
• At Primary 1-3, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.

1.4.b Assessing risks
• In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. 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 C2k can accept liability for the material accessed, or any consequences of Internet access.
• The headteacher will ensure that the e-Safety Policy is implemented and compliance with the policy monitored.

1.4.c 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 head teacher.
• Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

1.4.d Community use of the Internet
• Any community use of the internet through evening courses etc must be treated as if it were pupils using the network and as such must sign an 'E-Safety Agreement Form For Pupils'.

1.5 Communication of this Policy
1.5.a Introducing the e-safety policy to pupils
• Rules for Internet access will be posted in all networked rooms. (Appendix 4)
• Pupils will be informed that Internet use will be monitored.

• E-Safety lessons will be introduced at the beginning of the year to raise the awareness and importance of safe and responsible internet use. This will be part of our PSHE curriculum.

1.5.b 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.

1.5.c Enlisting parents' support

• Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and will be available to read on the school website.
www.holycrossboys.com

1.6 School usernames and Passwords

1.6.a Teachers' Usernames and Passwords

• At no point should a teacher share with anyone their personal username or password in order to safeguard their internet use and e-mail security.

• Anyone found using a teacher's username and password that is not that teacher shall be dealt with by the school principal.

• If you suspect your account has been accessed by another person you must report it to the E-Safety coordinator at once.

1.6.b Students' Usernames and Passwords

• In KS1 & KS2 all students are expected to log on using their individual username and password.

• In some instances when the teacher deems necessary, a generic username/classuser and password may be used for group tasks and whole class collaborations

• Any pupil found giving out or using another child's username and password will be dealt with by the principal.

• If you suspect your account has been accessed by another person you must report it to the E-Safety coordinator at once.

Student / Pupil Acceptable Use Policy Agreement

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:
• that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
• that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
The school will try to ensure that students / pupils will have good access to ICT to enhance their learning and will, in return, expect the students / pupils to agree to be responsible users.

Acceptable Use Policy Agreement
I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.
For my own personal safety:
• I understand that the school will monitor my use of the ICT systems, email and other digital communications.
• I will treat my username and password like my toothbrush – I will not share it, nor will I try to use any other person's username and password.
• I will be aware of "stranger danger", when I am communicating on-line.
• I will not disclose or share personal information about myself or others when on-line.
• If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
• I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:
• I understand that the school ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
• I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
• I will not use the school ICT systems for on-line gaming, on-line gambling, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.
• I will not steal, disable or cause any damage to school equipment, or the equipment belonging to others.

I will act as I expect others to act toward me:
• I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
• I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
• I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:
• I will only use my personal hand held / external devices (USB devices etc- mobile phones are not allowed) in school if I have permission. I understand that, if I do use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.

• I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

• I will immediately report any damage or faults involving equipment or software, however this may have happened.

• I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.

• I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.

• I will only use chat and social networking sites with permission, at the times that are allowed and with teacher supervision.

When using the internet for research or recreation, I recognise that:

• I should ensure that I have permission to use the original work of others in my own work

• Where work is protected by copyright, I will not try to download copies (including music and videos)

• When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

• I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).

• I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

PARENTAL PERMISSION FOR PHOTOGRAPH/RECORDING USE

This form relates to the use of recordings and photographs of the children who attend and who have attended Holy Cross Boys' Primary School.

The recordings/photographs will only be used for school use and promotion, such as:

- **The school website and social media accounts**

- **To illustrate school literature (eg school prospectus)**

- **Articles about the school in local media (sporting events, competitions, visits)**

- **Displays around the school**

- **Newsletters**

Please complete the sections below to show that you have read and understand and agree to allow Holy Cross Boys' Primary School to use photographs and recordings of your child for school purposes. This permission will cover your child's seven years at the school.

Name of Pupil: _____

Class: _____

Parental signature: _____

Date: _____

Staff (and Volunteer) Acceptable Use Policy Agreement

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

• that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
• that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
• that staff are protected from potential risk in their use of ICT in their everyday work.
The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for students / pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

• I understand that the school will monitor my use of the ICT systems, email and other digital communications.
• I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, VLE etc) out of school. (schools should amend this section in the light of their policies which relate to the use of school systems and equipment out of school)
• I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
• I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
• I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

• I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
• I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
• I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
• I will only use chat and social networking sites in school in accordance with the school's policies. (schools should amend this section to take account of their policy on access to social networking and similar sites)
• I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.

• I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

• When I use my personal hand held / external devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

• I will use personal email addresses very carefully on the school ICT systems and never allow the computer to save my password.

• I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.

• I will ensure that my data is regularly backed up, in accordance with relevant school policies.

• I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

• I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

• I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this has been allowed by the ICT coordinator.

• I will not disable or cause any damage to school equipment, or the equipment belonging to others.

• I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy (or other relevant school policy). Where personal data is transferred outside the secure school network, it must be encrypted.

• I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.

• I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

• I will ensure that I have permission to use the original work of others in my own work

• Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:

• I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.

• I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Teacher/Volunteer Name	
Signature	
Date	

PARENT/CARER ACCEPTABLE USE OF ICT POLICY AGREEMENT

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:
- That young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will ensure that pupils will have good access to ICT to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

As the parent/carer of the above pupil, I give permission for my son to have access to the internet and to IT systems at school. I know that my son will receive e-safety education to help them understand the importance of safe use of ICT – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about possible breaches of the Acceptable Use Policy. I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

You can view the E-Safety Policy on the school website at www.holycrossboys.com
This permission will cover your child's seven years at the school.

Name of Pupil: _____

Class: _____

Parental signature: _____

Date: _____

Holy Cross Boys' P.S.

Rules for Internet Use

- Ask permission before using the Internet.

- Only use your own network login and password.

- Do not bring software or disks into school without permission.

- Do not ignore pop up boxes you do not understand.

- Only e-mail people you know, or your teacher has approved.

- Messages you send must be polite and sensible. Emails containing offensive language will be filtered and blocked. However, it is your responsibility to ensure everything you send is appropriate.

- Keep your mailbox below 50Mb.

- Do not open e-mails/attachments from someone you do not know. Inform a teacher.

- You must never give out personal details; home address, telephone number.

- If you see anything you are unhappy with or receive messages you do not like, tell a teacher immediately.

- You must not search for offensive material.

- The school may check your computer files and Internet sites you visit.

- Deliberately breaking these rules may result in you not being allowed to use the Internet or computers.

You must only use <u>your</u> C2k email account