HOLY ROSARY CATHOLIC PRIMARY SCHOOL

E-SAFETY 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 safeguards and awareness for users to enable them to control their online experiences.

The school's e-safety policy will operate in conjunction with other policies including those Behaviour & Discipline, Anti Bullying, Computing, Safeguarding, Data Protection, Acceptable Use Policy and the Staff Code of Conduct.
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 school network design and use.
- Safe and secure broadband including the effective management of filtering.

Teaching and Learning
The importance of the Internet and digital communications

- Internet use is a part of the statutory curriculum and 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 pupils 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.
- 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 pupils who show a responsible and mature approach to its use.

The benefits of the Internet to education
Benefits of using the Internet in education include:

- Access to world-wide educational resources including museums and art galleries
- Inclusion in the National Education Network which connects all UK schools
- Educational and cultural exchanges between pupils world-wide
- Vocational, social and leisure use in libraries, clubs and at home
- Access to experts in many fields for pupils and staff
- Professional development for staff through access to national developments, educational materials and effective curriculum practice
- Collaboration across networks of schools, support services and professional associations
- Improved access to technical support including remote management of networks and automatic system updates
- Exchange of curriculum and administration data
- Access to learning wherever and whenever convenient

Internet use to enhance learning
The school's Internet access is 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 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 will guide pupils to on-line activities that will support the learning outcomes planned all pupils.
- 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.

Information system security

- 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 or otherwise secured.
- Unapproved software will not be allowed in network or other computer work areas.
- Files held on the school's network will be regularly checked for viruses and unauthorised software.
- The IT Leader / network manager will review system capacity regularly.
- The use of user logins and passwords to access the school network will be enforced.

Email

- Pupils and staff should only use e-mail addresses that have been issued by the school for school related matters.
- Pupils and staff are advised to maintain an alternative personal e-mail address for use in non-school related matters.
- Pupils must immediately tell a teacher if they receive an offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone that they do not know in real life.

Publishing pupil's images and work

- Pupils' full names will not be used in association with photographs.
- Parents and carers are permitted to take photos/videos of their own children in school events. They are requested not to share photos/videos from school events on social networking.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.

Social networking and personal publishing

- Staff must not communicate with students using public social networking sites such as Facebook, MySpace, Twitter, etc
- The school/LA will block/filter access to inappropriate 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 official blogs 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.
- 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.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- 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, particularly when concerning students' underage use of sites.
- 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 staff code of conduct/Acceptable Use Policy.

Mobile phones and personal devices

Electronic devices of all kinds that are brought into school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by such devices either potential or actual.

Pupil Use

- It is recognised that there may be situations where parents/carers want their children to carry a mobile phone, particularly in Year 6 where children may be walking to and from school alone. In these circumstances parents/carers must write and request permission for their child to bring their phone onto school premises.
- All mobile phones must be handed in to the office upon entry to school. Phones will be returned to the pupils at the end of the school day.
- Any child found in possession of a phone during the school day will have the phone taken to the office and it will be returned to the parents/carers.

- If a member of staff suspects that a mobile phone has been misused within the school then it should be confiscated and passed directly to SLT who will deal the matter in line with normal school procedures.

Staff Use

- Mobile Phone and devices will be switched off or switched to 'silent' mode and should not be used during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- In the EYFS department all mobile phones must be stored away within the setting during contact time with children (this includes staff, visitors, parents, volunteers and students).
- Nursery have a school mobile telephone. All telephone contact with Parents/Carers must be made on this telephone or that in the main office of the school.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Managing filtering

- The school will work in partnership with the LA and E-Safety committee to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site it must be reported.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- The school's broadband access will include filtering appropriate to primary school pupils.
- The school will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal will be reported to appropriate agencies.
- The school's access strategy will suit the age and curriculum requirements of the pupils.

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 sending of abusive or inappropriate files or messages utilising any form of electronic communication technology is forbidden.
- Staff will be issued with a school digital camera or other mobile device with an integral camera, such as an iPad or Tablet, where it is necessary to capture photographs of pupils.
- Photographs taken stored on school digital devices must only be uploaded to the school network or staff laptop.

Protection of personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Authorising Internet access

All staff must read and sign the 'Staff Code of Conduct' before using any school ICT resource.

- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- Parents and pupils will be asked to sign and return a consent form for acceptable use.
- All staff and student teachers must read and sign the 'Staff /Student Teacher Acceptable Use Policy before using any school IT resource.
- At Key Stage 1 and Early Years Foundation Stage, access to the Internet will be by adult demonstration followed by supervised access to specific, approved on-line materials.
- At Key Stage 2, staff will guide pupils in on-line activities that support the planned learning intentions. All internet access will be supervised by staff.

Assessing risks

- 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 LA can accept liability for the material accessed, or any consequences resulting from Internet use.
- The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches may be reported to Police.
- Methods to identify, assess and minimise risks will be reviewed regularly.

Handling Incidents of Concern

- 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 Leader will record all reported incidents and actions taken in the School e-Safety incident log and in any other relevant areas e.g. Behaviour log 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 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 learned 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 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 schools in LA.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a member of SLT in the first instance. If appropriate, the matter will then be dealt with under the School's complaints procedure.
- Any complaint about staff misuse must be referred to the Headteacher.
- All e-safety complaints and incidents will be recorded by the school in the e-safety incident log that is kept locked in the SLT office. The details of the user, date and incident should be reported.
- In the event of an e-safety complaint involving the Headteacher, the complainant should report directly to the Chair of Governors.
- Parents/carers and pupils will work in partnership with staff to resolve issues.
- Pupils and parents/carers will be informed of consequences for pupils misusing the Internet.
- Any issues (including sanctions) will be dealt with according to the school's Behaviour Policy 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.

Internet use across the community

The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking and social media sites, and offer appropriate advice in-line with this e-safety policy.

Managing Cyberbullying

Cyberbullying will not be tolerated in school. All incidents of cyberbullying will be recorded. Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's e-safety ethos.

There will be clear procedures in place to investigate incidents or allegations of cyberbullying:
a) Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
b) The school will take steps to identify the bully, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the police, if necessary.

Sanctions for those involved in cyberbullying may include:
a) The bully will be asked to remove any material deemed to be inappropriate or offensive.
b) Offensive content will be removed.
c) Internet access will be suspended at school for the user for a period of time.
d) Parent/carers will be informed.

e) The Police will be contacted if a criminal offence is suspected.

Support will be provided for anyone affected by cyberbullying. The school will become involved in incidents of cyberbullying which take place outside of school, when the effects of the cyberbullying overspill into school life, for example, when a child is upset in school. When that happens, the school will talk to the children involved and their parents, if it is deemed necessary.

Introducing the e-safety policy to pupils

- e-safety rules will be posted in all networked rooms.
- Users will be informed that network and Internet use will be monitored.
- The safe, responsible and respectful use of technology is part of the Computing curriculum for every year group and is detailed in the medium term plans
- E-safety instruction will cover both safe school and home use.
- Safe and responsible use of the internet and technology will be reinforced across the curriculum.
- Particular attention will be given where pupils are considered to be vulnerable.

Staff and the e-Safety policy

- The e–Safety Policy will be formally presented to and discussed with all members of staff.
- To protect all staff and pupils, the school will implement Acceptable Use Policies.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues.
- Staff training in safe and responsible internet use both professionally and personally will be provided.
- Staff will always use a child friendly safe search engine when accessing the web with pupils or performing an internet search where it is visible to pupils.
- Staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- Staff will change passwords regularly
- Staff must never let children use staff log on unsupervised
- Staff must risk assess any data that is removed from school, to ensure that any potential loss has minimal impact
- Encrypted USB pens are used in school (when necessary)

Health and Safety

In line with the school's Health and Safety policy, children are instructed in the safe use of all equipment.
Annual Portable Appliance Testing will be carried out on all portable equipment.

Equal opportunities

There is a school equal opportunities policy which is applied to computer use, internet access and all areas associated with other emerging technologies.

Disability and Discrimination Act

The Computing Leader and class teachers will ensure that resources used on school ICT systems do not reflect a negative stereotype of any particular group. The Computing Leader and class teachers will ensure equality of opportunity and access for all pupils.

E-Safety Committee

The school safety committee is convened by the e-safety officer. It will meet once per term and will invite a representative of the following groups: SLT, governors, teaching staff, admin staff, parents, pupils.

March 2016

AUP for learners in KS1

I want to feel safe all the time.

I agree that I will:

- Always keep my passwords private
- Only open pages which my teacher has said are OK
- Tell my teacher if anything makes me feel scared or uncomfortable on the internet
- Make sure all messages I send are polite
- Show my teacher if I get a nasty message
- Not reply to any nasty message or anything which makes me feel uncomfortable
- Only email people I know or if my teacher agrees
- Only use my school email address in school
- Not tell people about myself online (I will not tell them my name, anything about my home and family and pets)
- Not upload photographs of myself in school without asking a teacher
- Never agree to meet a stranger

I know that anything I do on the computer in school may be seen by someone else.

Signed _____ ***Printed _____***

AUP for learners in KS2

When I am using the computer or other technologies, I want to feel safe all the time.

I agree that I will:

- Always keep my password private
- Only visit sites which are appropriate
- Work in collaboration only with people my school has approved and will deny access to others
- Respect the school network security
- Make sure all messages I send are respectful
- Show a responsible adult any content that makes me feel unsafe or uncomfortable
- Not reply to any nasty message or anything which makes me feel uncomfortable
- Not use my own mobile device in school unless I am given permission
- Only email people I know or approved by my school
- Only use the email address provided by school, in school hours unless told otherwise
- Always follow the terms and conditions when using a site
- Always keep my personal details private (my name, family information, journey to school, My pets and hobbies are all examples of personal details)
- Only create and share content that is legal
- Not upload photographs of myself in school without asking a teacher
- Never agree to meet a stranger

I know that anything I share online may be monitored.

I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

Signed _____ Print Name _____

AUP for Parents

Holy Rosary Primary School

Pupil name: ……..

Pupil's registration class: ……

As the parent or legal guardian of the above pupil(s), I grant permission for my child to have access to use the Internet, the Virtual Learning Environment, school Email and other ICT facilities at school. I know that my child has signed a form to confirm that they will keep to the school's rules for responsible ICT use, outlined in the Acceptable Use Policy (AUP). I also understand that my child may be informed, if the rules have to be changed at any time.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using a filtered internet service, secure access to email, employing appropriate teaching practice and teaching e-safety skills to pupils.

I understand that the school can check my child's computer files, and the Internet sites they visit. I also know that the school may contact me if there are concerns about my child's e-safety or e-behaviour. I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety.

I am aware that the school permits parents/carers to take photographs and videos of their own children in school events and that the school requests that photos/videos are not shared on any social networking site such as Facebook. I will support the school's approach to e-Safety and will not upload or add any pictures, video or text.

Parent's signature:…… **Date:**…….