St Mary's Catholic Primary School
E-Safety Policy

The Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body / Board has taken on the role of E-Safety Governor.

The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Officer
- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors / Board / committee / meeting

Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community. Day to day responsibility for e-safety will be delegated to the E-safety Officer;
- The Headteacher and at least one other member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff;
- The Headteacher / Senior Leaders are responsible for ensuring that the E-Safety Coordinator / Officer and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

E-Safety Officer:

- leads the e-safety committee;
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents;
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place;
- provides training and advice for staff;
- liaises with the Local Authority / relevant body;
- liaises with school technical staff;
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments;
- meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs;
- attends relevant meeting / committee of Governors;
- reports regularly to Senior Leadership Team.

Teaching and 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;
- Planned workshops and events for pupils will take place throughout the year;

- The vast majority of 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.

Benefits of using the Internet in education include:

- access to worldwide educational resources including museums and art galleries;
- educational and cultural exchanges between pupils worldwide;
- 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 with Medway and DfE.

How the Internet can 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 school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law;
- Access levels will be reviewed to reflect the curriculum requirements and age of pupils;
- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and maturity;

- 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.

How pupils learn how to evaluate Internet content:

- An e-safety introduction will take place at the beginning of each IT lesson;
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy;
- The evaluation of online materials is part of teaching/learning in every subject.

Managing Information Systems 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;
- Unapproved software will not be allowed;
- Files held on the school's network will be regularly checked;
- The Computing Subject Leader and IT Technician will review system capacity regularly;
- The use of user logins and passwords to access the school network will be enforced.

The management of email:

- Pupils may only use approved email accounts;
- Pupils must immediately tell a teacher 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;
- Access in school to external personal email accounts may be blocked;

- Excessive social email use can interfere with learning and will be restricted;
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
- The forwarding of chain messages is not permitted;
- Staff should only use school email accounts to communicate with pupils, and then, only as part of learning activities;
- Staff should not use personal [non-Medway] email accounts during school hours or for other professional purposes.

The management of published content:

- The contact details on the website should be the school address, email and telephone number Staff or pupils' personal information must not be published;
- Staff and pupil email addresses should not be published;
- The website should comply with the school's guidelines for the publication of images including respect for intellectual property rights and copyright.

Publishing images and work:

- Images or videos that include pupils will be selected carefully and will not provide material that could be reused [images are locked];
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs – unless a parent specifically agrees to this publication;
- Written permission from parents or carers will be obtained before images of pupils are electronically published;
- Pupils work can only be published with their permission or that of their parents.

The management of social networking, social media and personal publishing:

- The school will control access to social media and social networking sites;
- Pupils will be advised on E-Safety and told never to give out personal details of any kind that 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. They will be

informed of the age restrictions that apply to social networking sites but that these are not policed;

- Pupils should be advised not to place personal photos on any social network space;
- They should consider how public the information is and consider using private areas;
- Advice should be given regarding background detail in a photograph that could identify the pupil or his/her location e.g. photographs with the school badge visible;
- Staff official blogs or wikis should be password protected and run from the school website with approval from the Senior Leadership Team;
- Staff should be advised not to run social network spaces for pupil use on a personal basis;
- If personal publishing is to be used with pupils then it must use age appropriate sites suitable for educational purposes;
- Personal information must not be published and school staff should moderate the site;
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications;
- Pupils should be encouraged to invite known friends only and deny access to others by making profiles private;
- Pupils are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory towards another person;

Filtering:

- The school will work with Medway to ensure that systems to protect pupils are reviewed and improved;
- If staff or pupils discover unsuitable sites, the URL must be reported to the IT Technician and E-Safety Officer;
- The school's broadband access will include filtering appropriate to the age and maturity of pupils;
- The IT Technician will manage the configuration of our filtering as far as possible but Medway will administer a general filtering policy for all schools. This task requires both educational and technical experience;

- The IT Technician along with the E-Safety Officer 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 must be reported to appropriate agencies such as 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 video conferencing equipment in the classroom must be switched off when not in use and not set to auto answer;
- External IP addresses should not be made available to other sites;
- Video conferencing contact information should not be put on the school website;
- The equipment must be secure and if necessary locked away when not in use;
- School video conferencing equipment should not be taken off school premises without permission.

Users:

- Pupils should ask permission from the supervising teacher before making or answering a video conference call;
- Video conferencing should be supervised appropriately for the pupils' age;
- Parents and carers should agree for their children to take 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.

Content:

- When recording a video conference 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;
- Video conferencing is a challenging activity with a wide range of learning benefits;
- Preparation and evaluation are essential to the whole activity;
- If third party materials are to be included, check that recording is acceptable to avoid infringing the third-party intellectual property rights;
- Establish dialogue with other conference participants before taking part in a video conference. If it is a non-school site it is important to check that they are delivering material that is appropriate for your class.

Emerging Technologies:

- 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.

Data Protection:

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2003. The eight principles are that personal data must be:
- Processed fairly and lawfully;
- Processed for specified purposes;
- Adequate, relevant and not excessive;
- Accurate and up-to-date;
- Held no longer than is necessary;
- Processed in line with individual's rights;
- Kept secure;
- Transferred only to other countries with suitable security measures.

Internet Access:

- The school will maintain a current record of all pupils who are not granted access to the school's electronic communications;

- Pupils will be allowed Internet access individually by agreeing to comply with the E–Safety Rules on entry to the school;
- Parents will be asked to sign and return a consent form for pupil to access sites;
- Parents will be informed that pupils will be provided with supervised Internet access on entry to the school;
- 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).

Managing Risk:

- 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 Medway can accept liability for the material accessed, or any consequences resulting from Internet use;
- The E-Safety Officer and ICT Technician will audit ICT use to establish if the E–Safety policy is adequate and that the implementation of the E–Safety policy is appropriate;
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990;
- Methods to identify, assess and minimise risks will be reviewed regularly.

Handling Complaints:

- All members of the school community will be informed about the procedure for reporting E-Safety concerns (such as breaches of filtering, cyber bullying, illegal content etc);
- The E-Safety Officer will record all reported incidents and actions taken;
- The Designated Safe Guarding Lead 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 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 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 Local Authority 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 Medway.

Cyber-bullying:

- Cyber-bullying (along with all forms of bullying) will not be tolerated in this school (Full details are set out in the school's policy on anti-bullying);
- There will be clear procedures in place to support anyone affected by Cyberbullying;
- All incidents of cyber-bullying reported to the school will be recorded;
- There will be clear procedures in place to investigate incidents or allegations of Cyber-bullying;
- Pupils, staff and parents/carers will be advised to keep a record of the cyberbullying as evidence;
- The school will take steps to identify the bully, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary;
- Sanctions for those involved in Cyber-bullying may also include:
    - The bully will be asked to remove any material deemed to be inappropriate or offensive;
    - A service provider may be contacted to remove content;
    - Internet access may be suspended at school for the user for a period of time;
    - Parent/carers may be informed;
    - The Police will be contacted if a criminal offence is suspected.

Management of mobile phones and personal devices:

- 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;
- Pupils must receive permission to have a mobile phone in school and mobiles must be handed to the class teacher on arrival into school;
- School staff may confiscate a phone or device if they believe it is being used to contravene the school's 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;
- Electronic devices of all kinds that are brought in to 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 any such devices either potential or actual.

Pupils Use of Personal Devices:

- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school policy;
- Phones and devices must not be taken into examinations. Pupils found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the pupil being withdrawn from either that examination or all examination;
- If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office;
- Pupils should protect their phone numbers by only giving them to trusted friends and family members;
- Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

Staff Use of Personal Devices:

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity;
- Mobile Phone and devices will be switched off or switched to 'silent' mode during lessons, Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by the Headteacher;
- If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity then it will only take place when approved by the Senior Leadership Team;
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils unless permission is given by the headteacher and these should be deleted at the earliest opportunity if permission is granted. Ideally staff should only use work-provided equipment for this purpose;
- If a member of staff breaches the school policy then disciplinary action may be taken.

  (cf: other information included in the Mobile Device Policy)

Communication of the policy:

Pupils:

- All users will be informed that network and Internet use will be monitored;
- Pupil instruction regarding responsible and safe use will precede 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.

Staff:

- The E–Safety Policy will be formally provided to and discussed with all members of staff;
- To protect all staff and pupils, the school has produced and will implement a Staff Acceptable Use Policy;

- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential;
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff;
- Staff who manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues;
- All members of 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.

Parent support:

- Parents' attention will be drawn to the School's E–Safety Policy in newsletters, the school brochure and on the school website;
- A partnership approach with parents will be encouraged. This may include parent evenings with demonstrations and suggestions for safe home Internet use or highlighting E–Safety at other attended events e.g. parent evenings, sports days;
- Parents will be requested to sign an E–Safety/internet agreement as part of the Home School Agreement;
- Information and guidance for parents on E–Safety will be made available to parents in a variety of formats;
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.