St. Raphael's Catholic Primary School E-Safety Policy
Purpose of the policy

- To ensure that whilst recognising the tremendous benefits technologies can have we are aware of the inherent safety concerns and dangers.
- To make users in the school community aware of the possible issues and concerns so that they can adopt safe practices and behaviours
- Outline the procedures in place to protect users and outline sanctions to be imposed if these are not Followed

Agreed Procedures for using the Shared Network

St Raphael's has a shared network which is accessible from any machine or laptop in the school. Teaching staff can also access the network remotely.

- Users must access the network using their own logons. All staff have a password. These must not be disclosed or shared.
- Staff will be regularly updated on e-safety procedures.
- New staff and trainees will receive e-safety training as part of their induction and will be asked to sign the Acceptable Use Policy (contained in the staff handbook)
- Users must respect confidentiality and attempts should not be made to access another individual's personal folder on the network without permission.
- Staff should not install software without prior permission from the network technician or ICT co-Ordinator.
- Removable media (e.g. pen drives / memory sticks, CD-ROMs) must be scanned for viruses before being used on a machine connected to the network. Children will not use their own USB pen drives on school machines
- Staff will use encrypted USB pen drives
- Machines should not be left 'logged on' and unattended. If a machine is to be left for a short while, it must be 'locked.'
- Machines must be 'logged off' correctly after use and shut down at the end of sessions.
- The wireless network is encrypted to prevent outsiders from being able to access it.

Agreed Procedures for Use of the Internet and Email

▪ All staff and all Key Stage 2 users must sign an Acceptable Use Agreement before access to the Internet and email is permitted in the establishment.

▪ In Foundation and Key Stage 1 the children will be told orally about simple rules when using the internet. In Key Stage 2 Internet rules will be read and discussed with the class teacher.

▪ Users must access the Internet and email using their own logon / password and not those of another individual. Passwords must remain confidential and no attempt should be made to access another user's email account.

▪ The Internet and email must only be used for professional or educational purposes during class time. Outside normal class time appropriate internet use is permitted.

▪ Children must be supervised at all times when using the Internet and email.

"May God's love shine in our lives as we care and share and learn together."

- Safe Internet Rules and sanctions applicable if rules are broken will be clearly displayed in every room with Internet access.

- Accidental access to inappropriate, abusive, racist or homophobic material is to be reported without delay to the Senior Management Team and ICT co-ordinator and a note of the offending website address (URL) taken so that it can be blocked.

- Internet and email filtering software is installed to restrict access, as far as possible, to inappropriate or offensive content and to reduce the receipt of 'spam,' junk or unwanted correspondence. This is to be reviewed and updated regularly by Simply ICT Solutions. No filtering system is 100% effective so it is important to teach responsible and sensible behaviour..

- Internet and email use can be monitored by the Simply ICT Solutions in accordance with the Data Protection Act

- Email addresses assigned to individual children will not be in a form which makes them easily identifiable to others. ie. They will not include a child's name, only a number.

- Children must not disclose any information of a personal nature in an email or on the Internet. This includes mobile and home phone numbers, addresses, or anything else which might allow them to be identified.

- All emails sent should be courteous and the formality and tone of the language used appropriate to the reader. No strong or racist language will be tolerated. Sanctions, appropriate to the case, will be imposed on any users who break this code of conduct.

- Bullying, harassment or abuse of any kind via email will not be tolerated. Sanctions, appropriate to the case, will be imposed on any users who break this code of conduct.

- If users are bullied, or offensive emails are received in school, this must be reported immediately to the Senior Management Team and the Headteacher, as the Child Protection Officer for correct recording. Emails received should not be deleted, but kept for investigation purposes.

- Anti-virus software is used on all machines and this is regularly updated by Simply ICT Solutions to ensure its effectiveness.

- Children must seek permission before downloading any files from the Internet.

- Staff can download files from educational sites to aid planning and teaching. However staff should download files from the internet and check suitability before using them in class. Eg. Youtube files should be downloaded and checked for suitability. Youtube should not be used 'live' in the classroom and children should never have access to Youtube in school.

- All users will be made aware of Copyright law and will acknowledge the source of any text, information or images copied from the Internet.

- An e-safety programme will form part of the ICT and PSHE curriculum and will include work in the classroom and Assemblies.

Agreed Procedures for Use of Cameras, Video Equipment and Webcams

- Permission must be obtained from a child's parent or carer before photographs or video footage can be taken. A permission form will be included in the Foundation stage brochure. The Senior Management team and ICT co-ordinator will collate returns and maintain a list of any children for whom permission has been refused.

- Photographs or video footage will not name individual children and will be saved into a designated folder.

- Any adult using their own camera, video recorder or camera phone during a trip or visit must transfer and save images and video footage into a designated folder on a school computer upon their return. These will then be deleted from their own equipment when no longer required.

- If video conferencing equipment or webcams are used they must be switched off (disconnected) when not in use and the camera turned to face the wall.

- Webcams, if in use, must not be used for personal communication and should only be used with an adult present.

"May God's love shine in our lives as we care and share and learn together."

- Children and staff must conduct themselves in a polite and respectful manner when representing the school in a video conference or when corresponding via a webcam. The tone and formality of the language used must be appropriate to the audience and situation.

Agreed Procedures to ensure safety of the school website

- The school SLT, Business Manager and ICT co-ordinator are responsible for approving all content and images to be uploaded onto the school website prior to it being published.

- The school website is frequently checked by the Senior Management Team and ICT co-ordinator to ensure that no material has been posted, which might put children or staff at risk.

- Copyright and intellectual property rights must be respected.

- Permission must be obtained from parents or carers before any images of children can be uploaded onto the school website. This will be obtained through a permission letter included in the Foundation stage brochure.
  Names must not be used to identify individuals portrayed in images uploaded onto the school website. Similarly, if a child or member of staff is mentioned on the website, photographs which might enable this individual to be identified must not appear.

- When photographs to be used on the website are saved, names of individuals should not be used as file names.

- Any area of public noticeboards, forums or weblogs on the school website will be monitored regularly by the Senior Management Team and ICT co-ordinator to check that no personal information or inappropriate or offensive material has been posted. Any such incidents will be investigated and logged. Further action may be taken where necessary.

Agreed Procedures for using mobile phones and Personal Digital Assistants (PDAs)

- All staff are required to switch mobile phones off during lesson time.

- Personal phone calls should not be made or received in public areas eg. the staff room

- The taking of still pictures or video footage without the subject's permission is not allowed

Sanctions to be imposed if procedures are not followed

- Following an incident of a procedure not being adhered to the incident will be logged and Senior Management Team will speak to the person or persons involved to investigate the incident and will decide if further action will be taken. Sanctions, where necessary, may include;

- Letters may be sent home to parents or carers (if applicable).

- Users may be suspended from using the school Internet or email, etc. for a given period of time / indefinitely.

- Details may be passed on to the police in more serious cases.

- Legal action may be taken in extreme circumstances.

- Staff could face disciplinary action

Monitoring This Policy
This policy was adopted (on behalf of the Governing Body) by the Curriculum Standards subcommittee in January 2015 and will be reviewed in January 2016.

"May God's love shine in our lives as we care and share and learn together."