St. Anne’s Catholic Primary School

E-Safety Policy 2016

Section 1

Security Guidelines

1. Monitoring use of devices by Pupils

- Discussing with parents and children the rules for using computers in school
- Copies of ‘Acceptable Use Policy’ to be signed by parents and returned to school.
- Ensuring pupil use of all devices is 'visual', make sure there is a Teacher/TA present and monitoring use.
- Review the layout of the room to ensure there is good 'visibility' of laptop and i-pad activities.
- Ensure there is supervision at **all times**
- Publish the ‘Rules of ICT Use’ in all rooms where pupils may use a computer.
- Laptops and i-pads are not to be used by children during wet playtimes or lunchtimes unless they are fully supervised by a teacher or TA.

2. Monitoring Computer Use by Staff (especially in sensitive areas)

- Think carefully about the location of equipment.
- Ensure sensitive documents are stored in a secure area of the computer.
- Take care when disposing of paper output, CD's, computers etc that may contain sensitive or personal information.

3. System Backup

- Make sure the system is backed up regularly and checks are made to make sure that the backup has worked.
- Try to implement an automated system backup.
- Make sure the instructions for re-installing data or files from a backup are fully documented and readily available
- Use 'off-site' storage for backup where possible.
- Consider using different media as a secondary backup facility

4. Anti Virus Protection

- Always use an approved and recommended product
- Make sure there is a process to ensure it is regularly updated and ALL equipment is included, this is especially important for stand-alone PC's, laptops and PC's used at home
- Make sure there is a clear procedure for dealing with any actual or suspected infections
- Make sure the process for 'cleaning' infections is documented - this may involve requesting assistance from the County Council

5. Illegal or Inappropriate Use of the Network

- Make sure there are appropriate procedures in place for auditing access to the network and systems
- Users must respect the work of others, which might be stored in common areas on the system. Conversely, users should always try and store their files and data in their own secure area
- Ensure that there is no attempt to access or store inappropriate or offensive material
- Make sure that staff are aware of what is considered inappropriate or offensive material
- Regularly check the network for 'unauthorised' files
- If possible ensure auditing is performed both at the Management System level and also at the Operating System level

6. Internet Use / Filtering

- Obtain parental permission where appropriate
- Ensure parents and children have read and signed AUP and returned to school
- Ensure there is a clear process for reporting any access to inappropriate material
- Consider restricting specific functions such as the downloading of .exe files
- Publish safe guidelines
- Make sure Internet use is supervised

7. Email Use

- Make sure an Email Use policy has been adopted (section 2) and all Users have signed up to it
- Be clear about what is considered 'appropriate' use of email and language

8. Documentation

Ensure adequate documentation is available for

- The network infrastructure

- The network systems, hardware, software etc
- Administration procedures
- Housekeeping procedures
- Problem resolution

Ensure support disks, recovery disks, backups etc are available

9. Training

- Ensure there is adequate training for staff
- Arrange at least one E-safety awareness day each year
- Introduce 'good practice' guidelines where appropriate
- Consider restricting the hours of use or physical access to systems

10. Authentication / Operating System Level Security

- Consider using system policies to provide additional security
- Ensure there is a rigorous policy for approval / removal of Users
- Limit the number of Administrator and Manager accounts
- Only log on as Administrator or Manager when performing functions requiring this level of access, use an ordinary level User account where this is not required
- Set clear security levels on the network and ensure these are documented and followed
- Restrict access to applications and data areas where appropriate
- Consider using 'read only' access where possible

11. Network Review

- Monitor system downtime, ensure there are support arrangements in place to react to problems with critical equipment or infrastructure
- Monitor performance of the network - ensure there is a process in place to develop and upgrade the network infrastructure and equipment as necessary
- Monitor service disruption - ensure support arrangements are in place to resolve problems in a timely fashion
- Regularly review appropriate documents e.g. Computer Security policy, Email and Internet Use policies.
- Copyright and intellectual property rights must be respected.
- Review procedures for dealing with all security breaches or compromises, whether deliberate or innocent

12. School Website and social media

- Ensure passwords are kept securely and regularly updated

- Only post content that is appropriate and that cannot be seen as offensive
- Refrain from using the names of children where possible
- Check that parental permission has been granted before publishing photographs

Section 2

e-mail & Internet Use Rules and Good Practice for staff

The following guidelines tell you what is and what is not acceptable when you use Internet or e-mail services.

You should:

- check your e-mail inbox for new messages regularly;
- treat e-mail as you would a letter, remember they can be forwarded / copied to others;
- use caution when receiving or opening e-mails from unknown senders
- report any offensive or inappropriate e-mails to a member of the senior leadership team.
- only use websites that are secure when transferring sensitive data
- ensure that your e-mail account is logged off when you leave the room

You should not:

- send e-mails that contain any material that may be viewed as offensive or inappropriate.
- use language that may be seen as offensive or vulgar in e-mails
- use your school e-mail account for e-mails that are unrelated to school
- attempt to access any websites that could be viewed as offensive or inappropriate

Inappropriate or offensive material refers to any e-mails, websites or documents containing offensive comments about race, gender, age, sexual orientation, religious or political beliefs, national origin or disability. It can also refer to, but is not limited to, any material related to pornography, violence or drugs that is unsuitable for a school environment.

The school may exercise its right by electronic means to monitor the use of the school's computer systems, including the monitoring of web-sites, the interception of E-mails and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.

Section 3

Rules for ICT Use for any third party in school

The school computer system sometimes provides Internet access to third parties that are other than staff and students. This e-mail and Internet Use Good Practice statement will help protect third parties, students and the school by clearly stating what is acceptable and what is not.

- Access must only be made via the user’s authorised account and password, which must not be given to any other person.
- CD's or USB sticks must not be brought into school unless permission has been given.
- Copyright and intellectual property rights must be respected.
- Users must respect the work of others, which might be stored in common areas on the system. Conversely, users should always try and store their files and data in their own secure area
- Users are responsible for e-mail they send and must not send e-mails or attempt to access websites that contain any material that may be viewed as offensive or inappropriate.
- Users should report any offensive or inappropriate material or messages received. The report will be confidential and will help protect others.
- The school ICT systems may not be used for private business purposes, unless the Head teacher has given permission for that use.
- The security of ICT systems must not be compromised, whether owned by the school or by other organisations or individuals.
- Irresponsible use may result in the loss of Internet access.

Inappropriate or offensive material refers to any e-mails, websites or documents containing offensive comments about race, gender, age, sexual orientation, religious or political beliefs, national origin or disability. It can also refer to, but is not limited to, any material related to pornography, violence or drugs that is unsuitable for a school environment.

The school may exercise its right by electronic means to monitor the use of the school’s computer systems, including the monitoring of web-sites, the interception of e-mails and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school’s computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.

St. Anne’s Catholic Primary School

E-Safety Policy for children

Rules for ICT Use

We use the school computers and Internet connection for learning.
These rules will help us to be fair to others and keep everyone safe.

- I will ask permission before entering any Web site, unless my teacher has already approved that site.
- On a network, I will use only my own login and password.
- I will not look at, change or delete other people's files.
- I will not bring CD's or USB sticks to use in school without permission.
- I will only use the computers for schoolwork and homework.
- I will only e-mail people I know, or my teacher has approved.
- When sending e-mail, I will not give my home address or phone number, or arrange to meet someone.
- I will ask for permission before opening an e-mail or an e-mail attachment sent by someone I do not know.
- I will not use Internet chat or social media sites.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
- I know that the school may check my computer files and may monitor the Internet sites I visit.
- I understand that if I deliberately break these rules, I could be stopped from using the Internet or computers.

For children bringing mobile phones to school:

- I will only use my mobile phone before 9:00am and after 3:30pm.
- I will hand my mobile phone in before registration and collect it at 3:30pm
- I will not use my mobile phone on the school premises.

The school may exercise its right by electronic means to monitor the use of the school’s computer systems, including the monitoring of web-sites, the interception of E-mail and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school’s computer system is or may be taking place.