St Anne's Catholic Primary School
On-line safety Policy

At St. Anne's we 'offer our children a creative, challenging and broad curriculum. We want them to be enthusiastic about learning.' We want them to be enthusiastic about learning.' This policy applies to all members of St. Anne's Catholic Primary School community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of the school's ICT/Computing systems, both in and out of St. Anne's Catholic Primary School.

1 Introduction

1.1 The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at St. Anne's Catholic Primary School with respect to the use of IT/Computing based technologies.

- Safeguard and protect the children and staff of St. Anne's Catholic Primary School.

- Assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.

- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.

- Have clear structures to deal with online abuse such as online bullying which are cross referenced with other school policies.

- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

2 Principles

2.1 The main areas of risk for our school community can be summarised as follows:

Content

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse.
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites.
- Hate sites.
- Content validation: how to check authenticity and accuracy of online content.

Contact

- Grooming.
- Online bullying in all forms.
- Identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords.

Conduct

- Privacy issues, including disclosure of personal information.
- Digital footprint and online reputation.
- Health and well-being (amount of time spent online (Internet or gaming).
- Sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images).

2.2 ICT in the 21st Century has an all-encompassing role within the lives of children and adults.

New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet ;
- e-mail;
- Instant messaging (http://www.msn.com, http://info.aol.co.uk/) often using simple web cams;

- Blogs (an on-line interactive diary);
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player);
- Social networking sites (Popular www.myspace.com / www.piczo.com / www.bebo.com / http://www.hi5.com / http://www.facebook.com);
- Video broadcasting sites (Popular: http://www.youtube.com/);
- Chat Rooms (Popular www.teenchat.com, www.habbohotel.co.uk);
- Gaming Sites (Popular www.neopets.com, http://www.miniclip.com/games/en/, http://www.runescape.com/ / http://www.clubpenguin.com);
- Music download sites (Popular http://www.apple.com/itunes/ http://www.napster.co.uk/ http://www-kazzaa.com/, http://www-livewire.com/);
- Mobile phones with camera and video functionality;
- Mobile technology (e.g. games consoles) that are 'internet ready';
- Smart phones with e-mail, web functionality and cut down 'Office' applications.
- Ipads.

2.3 Creating a safe ICT/Computing learning environment includes three main elements at this school:

- Providing access to an effective range of technological tools;
- Agreeing and maintaining policies and procedures, with clear roles and responsibilities;
- Providing On-line Safety education assemblies/workshops for pupils, staff and parents.

3 Roles and Responsibilities

3.1 On-line Safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school. The head teacher ensures that the Policy is implemented and compliance with the policy monitored.

3.2 The responsibility for e-Safety has been designated to:

Our school On-line Safety Co-ordinator: Computing lead, ELT
The named Child Protection Officer: Headteacher

Role	Key Responsibilities
Headteacher	• To take overall responsibility for Online Safety provision. • To take overall responsibility for data and data security (SIRO). • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements e.g. LGfL. • To be responsible for ensuring that staff receive suitable training to carry out their Online safety roles and to train other colleagues, as relevant. • To be aware of procedures to be followed in the event of a serious e-safety incident. • To receive regular monitoring reports from the Online Safety Co-ordinator / Officer. • To ensure that there is a system in place to monitor and support staff who carry out internal Online safety procedures(e.g. network manager).
Online Safety Co-ordinator / Designated Child Protection Lead	• Takes day to day responsibility for Online safety issues and has a leading role in establishing and reviewing the school Online safety policies / documents. • Promotes an awareness and commitment to Online safeguarding throughout the school community. • Ensures that Online safety education is embedded across the curriculum. • Liaises with school computing technical staff. • To communicate regularly with SLT and the designated Online safety Governor / committee to discuss current issues, review incident logs and filtering / change control logs. • To ensure that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident.

Role	Key Responsibilities

	• To ensure that an Online safety incident log is kept up to date.
	• Facilitates training and advice for all staff.
	• Liaises with the Local Authority and relevant agencies.
	• Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:
	  • sharing of personal data
	  • access to illegal / inappropriate materials
	  • inappropriate on-line contact with adults / strangers
	  • potential or actual incidents of grooming
	  • Online bullying and use of social media.

Governors / Online safety governor	• To ensure that the school follows all current Online safety advice to keep the children and staff safe. • To approve the Online Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors / Governors Sub Committee receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor. • To support the school in encouraging parents and the wider community to become engaged in e-safety activities. • The role of the Online Safety Governor will include: • Regular review with the Online Safety Co-ordinator / Officer (including Online safety incident logs, filtering / change control logs).
Computing Curriculum Leader	• To oversee the delivery of the online safety element of the Computing curriculum. • To liaise with the online safety coordinator regularly.
Network Manager/Technician	• To report any online safety related issues that arise, to the Online safety coordinator. • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed. • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date). • To ensure the security of the school IT/Computing system. • To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices. • The school's policy on web filtering is applied and

Role	Key Responsibilities
	updated on a regular basis. • LGfL is informed of issues relating to the filtering applied by the Grid. • That he / she keeps up to date with the school's Online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant. • That the use of the Network / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Online Safety Co-ordinator / Officer /Headteacher for investigation / action / sanction. • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To keep up-to-date documentation of the school's online security and technical procedures.
LEARNING PLATFORM Leader (Computing Leader)	• To ensure that all data held on pupils on the Learning Platform (s) is adequately protected.
Data Manager	• To ensure that all data held on pupils on the school office machines have appropriate access controls in place.
LGfL Nominated contact(s)	• To ensure all LGfL services are managed on behalf of the school including maintaining the LGfL USO database of access accounts.
Teachers	• To embed online safety issues in all aspects of the curriculum and other school activities. • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant). • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.
All staff	• To read, understand and help promote the school's e-safety policies and guidance. • To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy. • To be aware of online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices.

Role	Key Responsibilities
	• To report any suspected misuse or problem to the online safety coordinator. • To maintain an awareness of current online safety issues and guidance e.g. through CPD. • To model safe, responsible and professional behaviours in their own use of technology. • To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.
Pupils	• Read, understand, sign and adhere to the Student / Pupil Acceptable Use Policy (**NB: KS1 it would be expected that parents / carers would sign on behalf of the pupils**). • Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • To understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology. • To know and understand school policy on the use of mobile phones, digital cameras and hand held devices. • To know and understand school policy on the taking / use of images and on cyber-bullying. • To understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school. • To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home. • To help the school in the creation/ review of e-safety policies.
Parent Liaison Officer	• Educating Parents and raising awareness as instructed by Head.

Role	Key Responsibilities
Parents/carers	• To support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images. • To read, understand and promote the school Pupil Acceptable Use Agreement with their children. • To access the school website / Learning Platform (s) / on-line student / pupil records in accordance with the relevant school Acceptable Use Agreement. • To consult with the school if they have any concerns about their children's use of technology.
External groups	• Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school.

4 Communications

4.1 How is the policy introduced to pupils and parents/carers?

Internet use in pupils' homes is increasing rapidly. Unless parents are aware of the dangers, pupils may have unrestricted access to the Internet. The school may be able to help parents plan appropriate supervised use of the Internet at home:

- On-line Safety workshop for parents & staff;
- On-line Safety assembly for children (based on Key Phase);
- Information to be provided for parents to take home;
- Internet issues will be handled sensitively, and parents will be advised accordingly;
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents;

- Use of the school's website and MLE to promote positive use of technology and internet use.
- Acceptable use agreements will be issued to whole school community, usually on entry to the school.

4.2 How is the policy discussed with staff?

ICT/computing use is widespread and all staff including administration, caretaker, governors and support staff should be included in appropriate awareness raising and training. Induction of new staff should include a discussion of the school's On-line Safety Policy.

- Policy will be part of school induction pack for new staff.
- Acceptable use agreements will be discussed with pupils at the start of each year.
- Acceptable use agreements will be held in pupil and personnel files.

5 Complaints Procedure

5.1 The school will take all reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

5.2 Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- Meeting with teacher, on-line safety co-ordinator, Head teacher;
- Informing parents or carers;
- Removal of Internet or computer access for a period;
- Referral to LA/Police in extreme cases.

5.3 Our on-line Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Head teacher.

5.4 Complaints of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy.

5.5 Complaints related to child protection are dealt with in accordance with school/LA child protection procedures.

6 Related policies

6.1 See also:

- Confidentiality;
- Health and safety;
- ICT;
- Staff code of conduct;
- Teaching and learning

Date agreed by Governing Body on	**Signature of Chair or Vice Chair**
Date agreed for review **Summer 2018**	**Frequency of Review** Annual/~~Bi-annual/Three-year cycle~~
Responsibility for Review Committee / Headteacher	

APPENDICES

1 Staff Code of Conduct
2 Email Policy
3 Managing equipment
4 Managing the Internet
5 On-line-Safety Home Guidelines
6 Parents Consent Letter and Rules
7 Pupil Rules Letter

Staff Information Systems Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's on-line safety policy for further information and clarification.

1 The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
2 I will ensure that my information systems use will always be compatible with my professional role.
3 I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
4 I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
5 I will not install any software or hardware, unless freeware or software updates onto the school network without permission.
6 I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
7 I will respect copyright and intellectual property rights.
8 I will report any incidents of concern regarding children's safety to the school e-Safety Coordinator/Designated Child Protection Coordinator.
9 I will ensure that any electronic communications with pupils are compatible with my professional role.
10 I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use and to the content they access or create.
11 I will ensure that devices used to store information (USB sticks) are stored in an appropriate way for safety/security reasons.
12 I will ensure that security settings on social networking sites are 'high', allowing only a name and an appropriate photo to be displayed.
13 I will use my School email address for work related items.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Information Systems Code of Conduct.

Signed: …… Capitals: …… Date: ……

St Anne's School:

1 Does not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous, group e-mail or our school/class MLE addresses for any communication with the wider public.

2 If one of our staff or pupils receives an e-mail that they find particularly disturbing or breaks the law we may contact the police.

3 Email accounts are managed effectively, with up to date account details of users

4 Messages relating to or in support of illegal activities may be reported to the authorities.

Pupils:

1 We only use an agreed safe email system with pupils.

2 Pupils should only use the e-mail accounts on the school system.

3 Pupils are introduced to, and use e-mail as part of the ICT/Computing scheme of work (Year 3).

4 Pupils are taught about the safety of using e-mail i.e.

a. not to give out their e-mail address unless it is approved by their teacher or parent/carer;
b. that an e-mail is a form of publishing where the message should be clear, short and concise;
c. that any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
d. they must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc;
e. to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
f. the sending of attachments should be limited;
g. that they must immediately tell a teacher/parent/carer if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature;
h. not to respond to malicious or threatening messages;
i. not to delete malicious of threatening e-mails, but to keep them as evidence of bullying;
j. not to arrange to meet anyone they meet through e-mail;
k. that forwarding 'chain' e-mail letters is not permitted;
l. Pupils sign the school Acceptable Use Policy to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Staff:

1 Staff use LA e-mail systems for professional purposes, however personal email is permitted for use during personal time within the school ensuring that contents will not be on display for the children at any time ;

2 Staff should be aware that e-mails sent to external organisations are written carefully, (and may require authorisation), in the same way as a letter written on school headed paper.

3 Staff sign the appropriate School Agreement Form to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

1: Using the school network, equipment and data safely: general guidance

The computer system / network is owned by the school and is made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management.

2: To ensure the network is used safely this school:

2.1 Ensures staff read and sign that they have understood the school's e-safety Policy. Following this, they are set-up with Internet and email access and can be given an individual network log-in username and password, email address and MLE Login;

2.2 Provides pupils with an individual network and MLE login. From Year 3 they are also provided with a school email and password;

2.3 Makes it clear that staff must keep their log-on username and password private and must not leave them where others can find;

2.4 Makes clear that pupils should never be allowed to log-on or use teacher/staff logins – as they have far less security restrictions and inappropriate use could damage files or the network;

2.5 Makes clear that no one should log on as another user, new staff/pupils will be added to the system with direction from the headteacher/classteacher;

2.6 Has set-up the network with a shared work area for pupils (RMShared) and one for staff (RMStaff). Staff and pupils are shown how to save work and access work from these areas;

2.7 Requires users to log off when they have finished working or are leaving the computer unattended, this practice should be encouraged with the children;

2.8 Has set up a automated shut down and start-up of computers;

2.9 Has set-up the network so that users have restricted access when downloading executable files / programmes;

2.10 Has allowed (internet provider) to block access to certain sites – allowing those approved for educational purposes;

2.11 Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used to support their professional responsibilities;

2.12 Maintains equipment to ensure Health and Safety is followed; e.g. projector filters cleaned; equipment installed and checked by approved electrical engineers;

2.13 Provides pupils and staff with access to content and resources through the approved Learning Platforms and MLE which staff and pupils access using their username and password;

2.14 Uses our broadband network for our CCTV system;

2.15 Follows LA advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;

2.16 Reviews the school ICT/Computing systems regularly with regard to security.

1: St Anne's School:

1.1 Maintains the filtered broadband connectivity;

1.2 Works in partnership with the LA to ensure any concerns about the system are communicated so that systems remain robust and protect students;

1.3 Has additional user-level filtering in-place using the **Synetrix** service

1.4 Ensures network health through appropriate anti-virus software and network set-up;

1.5 Uses individual log-ins for all pupils, parents, staff, students, supply teachers and other stakeholders;

2: Policy and procedures:

St Anne's School:

2.1 Supervises pupils' use at all times, as far as is reasonable, and is vigilant in learning resource areas where older pupils have more flexible access;

2.2 We use the LA recommended filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature;

2.3 Staff should preview all sites before use or only use sites accessed from managed 'safe' environments such as the Learning Platform (espresso), Managed Learning Environment;

2.4 Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required;

2.5 Informs users that Internet use is monitored;

2.6 Informs staff and students that that they must report any failure of the filtering systems directly to the ICT/Computing Co-ordinator and or the E-Safety Officer where necessary;

2.7 Requires pupils (and their parent/carer) from Key Stage 1 and 2, to individually sign an e-safety / acceptable use agreement form which is fully explained and used as part of the teaching programme;

2.8 Requires all staff to sign an e-safety Code of Conduct form and keeps a copy on file;

2.9 Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings;

2.10 Keeps a record, e.g. print-out, of any bullying or inappropriate behaviour for as long as is reasonable in-line with the school behaviour policy;

2.11 Ensures parents provide consent for pupils to use the Internet, as well as other ICT/Computing technologies, as part of the e-safety acceptable use agreement form at time of their daughter's / son's entry to the school;

2.12 Makes information on reporting offensive materials, abuse / bullying etc available for pupils, staff and parents;

2.13 Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

3: Education and training:

St Anne's School:

3.1 Fosters a 'No Blame' environment that encourages pupils to tell a teacher / responsible adult immediately if they encounter any material that makes them feel uncomfortable while at school;

3.2 Ensures pupils and staff know what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher or ICT/Computing Co-ordinator.

3.3 Ensures pupils and staff know what to do if there is a cyber-bullying incident, through assemblies and training annually;

3.4 Ensures all pupils know how to report abuse;

3.5 Has a clear, progressive e-safety programme, built on LA / London / national guidance in addition to objectives from the National Curriculum. Staff and pupils are taught a range of skills and behaviours appropriate to their age and experience, such as:

a. to THINK before they CLICK
b. to discriminate between fact, fiction and opinion;
c. to develop a range of strategies to validate and verify information before accepting its accuracy;
d. to skim and scan information;
e. to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
f. to know some search engines / web sites that are more likely to bring effective results;
g. to know how to narrow down or refine a search;
h. to understand how search engines work;
i. to understand why people they meet on-line may not be who they say they are;
j. to understand why they should not share personal contact information, and to know how to ensure they have turned-on privacy settings;
k. to understand why they must not post pictures or videos of others without their permission;

l. to have strategies for dealing with receipt of inappropriate materials;

3.6 Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright / intellectual property rights;

3.7 Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate.

3.8 Makes training available annually to staff, parents/carers and pupils on the e-safety program including:

a. Information leaflets; in school newsletters; on the school web site;
b. demonstrations, practical sessions held at school;
c. distribution of 'think u know' for parents materials
d. suggestions for safe Internet use at home;
e. provision of information about national support sites for parents.

Home and Family guidelines

- ☺ Talk together and have fun learning together.
- ☺ Involve everyone and agree your family guidelines and rules. Remember that sometimes what is acceptable for a Year 6 child is not necessarily acceptable for a Year 4 or Year 2 child.
- ☺ Discuss online safety regularly and go online **with** your children. **Communication is the key to on-line-Safety**.
- ☺ Keep virus and firewall software as up to-date as possible.
- ☺ Regularly check the history on the computer so that you can see what websites your child is on.
- ☺ Encourage the use of the school Managed learning environment (MLE) and child-friendly search engines (Google Junior, Kids You tube, Kid Rex, Swiggle).
- ☺ Keep the computer in a communal area of the house, where it's easier to monitor what your children are viewing. Never let children have webcams, or similar, in their bedroom.
- ☺ Talk to your children about why they should not give out their personal details. If they want to subscribe to any online service then make up a family email address to receive the mail.
- ☺ The time children spend offline following a range of other activities is equally important. Time spent online should be monitored to help prevent obsessive use of the internet
- ☺ Encourage your children to tell you if they feel uncomfortable, upset or threatened by anything they see online.

Key Stage 1

Think then Click

These rules help us to stay safe on the Internet

We only use the internet when an adult is with us

We can click on the buttons or links when we know what they do.

We can safely search the Internet.

We always ask if we get lost on the Internet.

We can send and open emails together.

We can write polite and friendly emails to people that we know.

Key Stage 2

Think then Click

On-line Safety Rules for Key Stage 2

- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we are not sure about.
- We only e-mail people an adult has approved.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not open e-mails sent by anyone we don't know.
- We do not use Internet chat rooms.

St Anne's Catholic Primary School
On-line Safety Rules for Children

All pupils use computer facilities including Internet access as an essential part of learning, as required by the ICT/Computing Curriculum. Both pupils and their parents/carers are asked to sign to show that the e-Safety Rules have been understood and agreed.

Pupil:	***Class:***

Pupil's Agreement

- I have read and I understand the school e-Safety Rules.
- I will use the computers, network, mobile phones, internet access and other new technologies in a responsible way at all times.
- I know that network and internet access may be monitored.

KS2 Child signature:	***Date:***

Parent's Consent for Web Publication of completed work

I agree that my child's work may be electronically published.

Parent's Consent for Internet Access

I have read and understood the school e-safety rules and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed:	***Date:***

Pupil Acceptable Use Agreement

Dear Parent/ Carer

ICT/Computing including the internet, email, laptops, digital cameras etc has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT/Computing.

Please discuss these On-line Safety rules with your child.

1. I will only use ICT/Computing in school for school purposes.
2. I will only use my class email address or my own school email address.
3. I will make sure that all ICT/Computing contacts with other children and adults are responsible.
4. I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will turn off my monitor and tell my teacher immediately.
5. I will not send to children or adults anything that could be considered unpleasant or nasty.
6. I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
7. I will be responsible for my behaviour when using ICT/Computing because I know that these rules are to keep me safe.
8. I know that my use of ICT/computing can be checked and that my parent/carer contacted if a member of school staff is concerned about my On-line Safety.

Parent/Carer signature

We have discussed this and …….....(child name) agrees to follow the On-line Safety rules and to support the safe use of ICT/Computing at St Anne's Catholic Primary School.

Parent/ Carer Signature ……

Class …… Date ……