St Anne's Catholic Primary School

E-safety policy 2018

Creation and Review	
Author(s)	(E-safety lead) Melanie Dobson (Computing co-ordinator)
Last Review Date	September 2018
Ratified by Governing Body	
Next Review Date	July 2019

Article 3: The best interests of the child must be a top priority in all actions concerning children

Contents page

Introduction

At St Anne's Catholic Primary School we are committed to ensuring that children learn how to use computers, ICT and modern technologies safely so that they:

- Are able to use ICT safely to support their learning in school.
- Know how to use a range of ICT equipment safely.
- Are able to use ICT and modern technologies outside school in a safe manner, including using ICT as a tool for communication.
- Are prepared for the constant changes in the world of technology and understand how to use new and emerging technologies in a safe manner.
- Know what to do if they feel unsafe when it comes to using technology and ICT.

This policy outlines the steps the school takes to protect children from harm when using ICT and also how the school proactively encourages children to develop a safe approach to using ICT whether in school or at home. (*See also appendix 1 – Incident workflow)*

The Law

Our E-Safety Policy has been written by the school, using advice from HCC and government guidance. The Policy is part of the school's Strategic Development Plan and related to other policies including Positive Learning, Safeguarding and Data Protection policies. As legislation is often amended and new regulations introduced the references made in this policy may be superseded. For an up to date list of legislation applying to schools please refer to the Department for Education website at www.education.gov.uk/schools.

Roles and Responsibilities

The Headteacher, alongside the E-safety officer (_____) will:

- Ensure the policy is implemented, communicated and compliance with the policy is monitored.
- Ensure staff training in e-safety is provided and updated annually as part of safeguarding training.
- Ensure immediate action is always taken if any risks or dangers are identified i.e. reporting of inappropriate websites.
- Ensure that all reported incidents of cyber bullying are investigated.
- Ensure appropriate web filtering software is used to protect users from potentially damaging/offensive material.

Teachers and Staff will:

- Keep passwords private and only use their own login details, which are stored securely.
- Monitor and supervise pupils' internet usage and use of other IT resources.
- Adhere to the Acceptable Use Agreement (*see appendix 3,4 & 5*).
- Promote e-safety and teach e-safety units as part of computing curriculum.
- Engage in e-safety training.
- Only download attachments/material onto the school system if they are from a trusted source.

- When capturing images, videos or sound clips of children, only use school cameras or recording devices.

It is essential that pupils, parents/carers and the public at large have confidence in the school's decisions and services. The principles set out in this policy are designed to ensure that staff members use social media responsibly so that confidentiality of staff members and the reputation of the school and the County Council are safeguarded. In this context, staff members must be conscious at all times of the need to keep their personal and professional lives separate.

Governors will:

- Ensure that the school is implementing this policy effectively.
- Adhere to the acceptable use agreement when in school.
- Have due regard for the importance of e-safety in school.

Teaching and Learning

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety is a focus in all areas of the curriculum and staff reinforce e-safety messages across the curriculum. The e-safety curriculum is broad, relevant and provides progression, with opportunities for creative activities and is provided in the following ways:

- A planned e-safety curriculum is provided as part of Computing / PHSE / other lessons and is regularly revisited
- Key e-safety messages are reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs,). *(Discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.*

Parents/ Guardians

Parents/Guardians play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Research shows that many parents and guardians do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through the school website, parent evenings and newsletters

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site
- Parents/ Carers evenings /sessions (Year 5/6)
- High profile events / campaigns e.g. Safer Internet Day and Cyberbullying day.
- Reference to the relevant web sites / publications e.g.

  www.swgfl.org.ukwww.saferinternet.org.uk/

  http://www.childnet.com/parents-and-carers

  www.thinkyouknow.co.uk (CEOP)

Parents/Guardians will be responsible for:

- supporting the school in promoting e-safety and endorsing the Parents' Acceptable Use Agreement (see Appendix 4 & 5) which includes the pupils' use of the Internet and the school's use of photographic and video images.
- reading, understanding and promoting the school Pupil Acceptable Use Agreement with their children.
- consulting with the school if they have concerns about their children's use of technology.

Monitoring safe and secure systems

Antivirus software has been installed on all computers and is to be maintained and updated regularly. Staff passwords are changed regularly and must be strong passwords. Staff take responsibility for safeguarding confidential data saved to laptops, i.e. use of strong passwords. If personal data has to be saved to other media, e.g. memory pens or external hard drives, it is to be encrypted or strong password protected. Staff with access to the ICT systems containing confidential and personal data are to ensure that such data is properly protected at all times. Teaching and support staff have access to google drive, this reduces the need for portable data storage and therefore increases security. G-drive is linked to staffs g-mail accounts and is fully password protected.

Pupils

It is important that all pupils at St Anne's:

- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.

- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's / academy's E-Safety Policy covers their actions out of school, if related to their membership of the school.

Communication

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website with hard copies available from school on request.
- Policy to be part of school induction pack for new staff.
- Acceptable use agreements discussed with pupils at the start of each year.
- Acceptable use agreements to be recorded by the office and kept in teacher files.

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the nominated person – in accordance with the school/ academy policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils (email on Purple Mash etc.) must be professional in tone and content. Personal email addresses, text messaging or social media must not be used for these communications.
- Students / pupils should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Approaches to Teaching and Learning

- Safety is embedded into the curriculum and is covered through Computing and PSHE objectives.
- Pupils need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Pupils will be expected to know school rules and understand school policies for bullying and behaviour, this is reinforced through class worship and Internet Safety Week.
- Pupils should understand the importance of adopting good e-safety practice when using digital technologies out of school.

Handling complaints

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.

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

- Interview with teacher/ Computing Subject Leaders/ SLT / Headteacher;
- Informing parents or carers;
- Removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including online homework];
- Referral to LA / Police.

Our _____ act as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school/ LA child protection procedures.

Review and Monitoring

The e-safety policy is referenced from within other school policies:

- The school has two Computing coordinators (Computing lead and E-safety lead) who will be responsible for document ownership, review and updates.
- The e-safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- The e-safety policy has been written by the school Computing Coordinators and is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school e-safeguarding policy will be discussed in detail with all members of teaching staff.

There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors and other stakeholders. All amendments to the school e-safeguarding policy will be discussed in detail with all members of teaching staff.

Planning and Organisation

E-safety should be focused upon in all areas of the curriculum and staff should reinforce e-safety messages during computing lessons. The Computing coordinator has a clear, progressive and up-to-date e-safety education programme as part of the Computing curriculum/E-safety curriculum. This covers a range of skills and behaviours appropriate to their age and experience (see Appendix 3).

In the Foundation Stage, pupils are taught to not give out any personal information on the internet. They are told to tell a teacher or parent if anything they see on the internet makes them feel uncomfortable. At St Anne's Catholic Primary School we do expect children of this age to be supervised whilst using the internet. Reception pupils take part in the school "Internet Safety Week" using age appropriate CEOP resources.

In Key Stage One, pupils begin to understand what personal information is and who you can share it with. Children begin to recognise the difference between real and imaginary online experiences. They are taught to keep their passwords private and make sure that an adult knows what they are doing online. Staff to use https://www.commonsensemedia.org/pause to highlight the need to be good digital citizens. Teachers model appropriate online behaviour when communicating with others.

There are four key messages taught at Key Stage One:

- People you don't know are strangers. They're not always who they say they are.
- Be nice to others on the internet, like you would on the playground.

- Keep your personal information private.
- If you ever get that 'uh-oh' feeling, you should tell a grown-up you trust.

In Key Stage Two, themes taught in Key Stage One are built upon. In addition, pupils are made aware of online experiences which could cause potential danger, e.g. use of social networking, gaming sites and downloading or installing new applications. Links are made between inappropriate sharing of personal information and the dangers this can pose in the real world. Relevant resources from CEOP, Childnet and SWGfL are used during "Internet Safety Week" and other resources can be accessed throughout the year on the school website. In Key Stage Two, children also develop their research skills, especially through use of their iPads. They are taught about plagiarism and the need to upload copyright laws.

Resources

The Computing coordinator will provide e-safety planning and resources for teachers to follow. Online websites links are available on the school website. Information about new resources/websites are communicated to staff via email.

Inclusion

At St Anne's we believe that all our children should be given the opportunity to achieve as well as they can in everything they do.

Acceptable Use of Personal Equipment - Children

Use of Facebook / Social networking sites

Children are not permitted to use social networking sites on school premises. Both on computers or mobile devices.

Use of Mobile Phones

Mobile devices must be switched off and remain in bags during the school day. Parents and pupils to sign a disclaimer form if they wish to bring a mobile device into school *(see Appendix 6)*.

Mobile phones brought into school are entirely at the staff member/ visitors' own risk. St Anne's Primary School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.

The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying.

Where parents or students need to contact each other during the school day, they should do so only through the School's telephone.

Email

Children currently use the closed messaging systems of Purplemash. Other messaging or e-mail solutions may be used when appropriate for a particular year group. This will be decided by the Computing coordinator and the Headteacher.

Cyber-Bullying

Internet Safety Week is held annually with up to date e-safety guidance. As part of Anti-bullying week, there is a specific day for school to focus on Cyberbullying (15th November), issues and ways to tackle cyberbullying will be revisited throughout the course of the year. The school website has links to cyber-bullying advice. Incidents of cyber-bullying are dealt with by leadership team and communicated to parents where necessary.

Acceptable Use Policy (AUP)

The AUP is written and distributed to all pupils (age appropriate) during the Autumn term of the school year and signed by parents/guardians. The AUP will be reviewed annually.

Acceptable Use of Personal Equipment - Staff

Use of Facebook / Social networking sites

Staff are not permitted to access facebook or other social networking sites from a school computer whilst on school premises. Social networking sites can be accessed on a personal handheld device at break, lunch times or the when children have left school. All staff social media accounts will be set to private, so only 'friends' can view their information.

Use of Mobile Phones and other personal mobile devices

- During the school day, mobile phones and other personal mobile devices can be accessed at break times only. Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by the Headteacher in emergency circumstances.
- If staff use their personal mobile phones to take pictures of children in school, these should be removed as soon as possible and kept password protected at all times.
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity. Staff will be issued with a school phone where contact with students, parents or carers is required.
- Staff iPads must have a 4 digit passcode activated.

Use of Cameras

- Images of pupils and/ or staff must only be stored on computers/drivers owned by the school. Images will not be distributed outside the school network (e.g. Website/local press) without the permission of the parent/ carer, member of staff or Headteacher.
- Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

- In accordance with guidance from the Information Commissioner's Office, parents/ carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy, these images should not be published/ made publicly available on social networking sites, nor should parents/ carers comment on any activities involving other students/ pupils in the digital/ video images.
- Photographs published on the website, or elsewhere that include students/ pupils will be selected carefully and will comply with good practice guidance on the use of such image.
- Written permission from parents or carers will be obtained before photographs of students/ pupils are published on the school website.

Email

Emailing is used as one of the many ways we communicate with each other at St Anne's Primary School and is invaluable in such a large school. However, the system should be used responsibly and staff should always act in a professional manner when using the email system. Members of staff should not feel obliged to reply to any emails sent to them in the evenings or at weekends and equally staff should not expect a reply from colleagues outside school hours.

Incident Management

In this school:

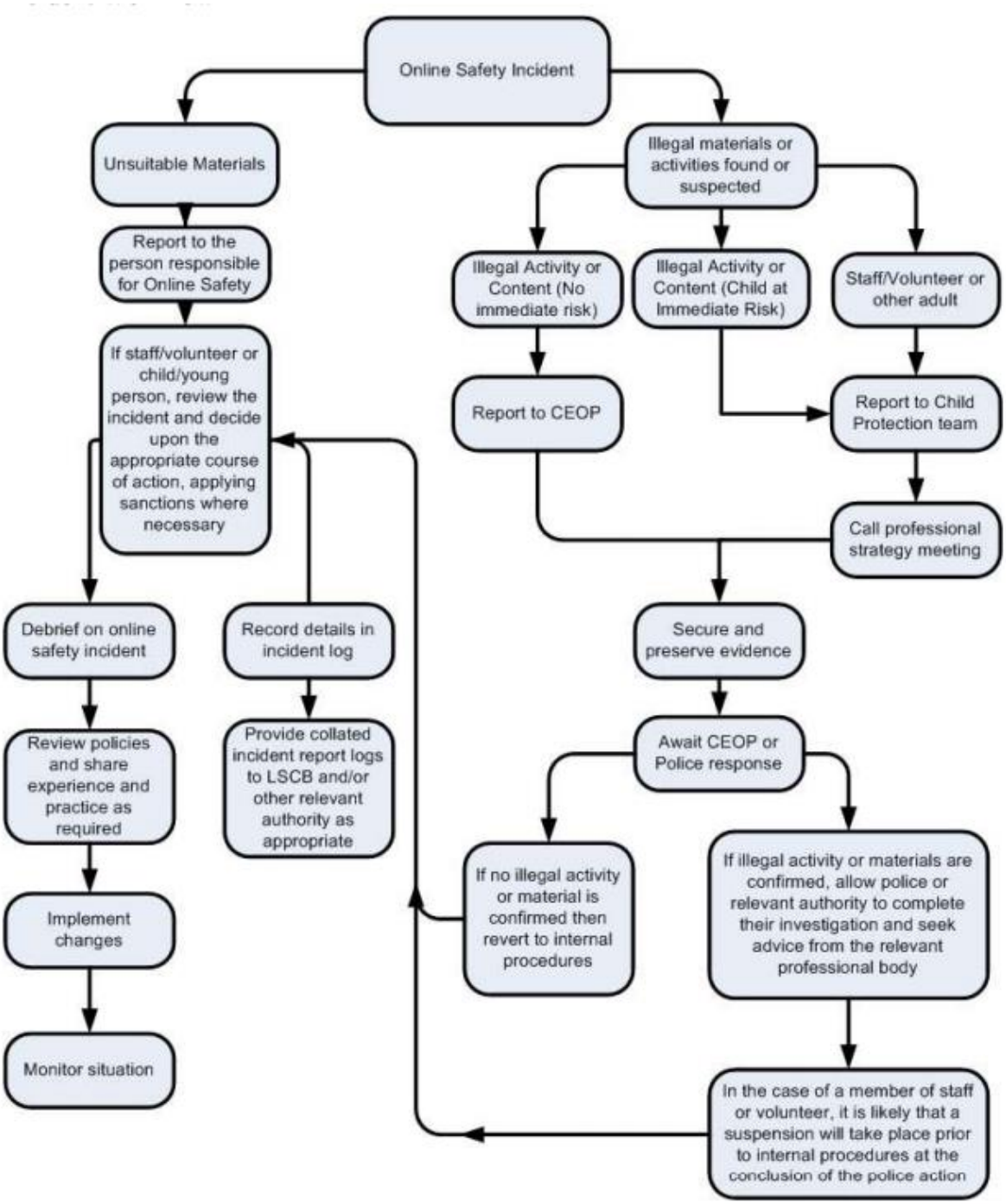
- there is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions
- all members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.
- support will be actively sought from other agencies as needed (e.g. the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with e-safety issues
- monitoring and reporting of e safety incidents takes place and contribute to developments in policy and practice in e-safety within the school.
- parents/ carers are specifically informed of e-safety incidents involving young people for whom they are responsible.
- we will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law
- any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's Computing Subject Leaders, Infrastructure Manager or Leadership Team.
- all security breaches, lost/stolen equipment or data virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the Computing Subject Leaders and Infrastructure Manager.

CCTV

We have CCTV in the school as part of our site surveillance for staff and student safety. This will be viewed where cause is justified (in line with the Behaviour Policy) and will only be viewed by the person leading the investigation.

APPENDIX 1

Incident workflow



APPENDIX 2:
(A more detailed progression grid for each year group is shared with teaching staff)

APPENDIX 3

St Anne's Catholic Primary School
Loving & learning together in Harmony with Christ

Staff Acceptable Use Policy

This policy covers the use of digital technologies in school: email, Internet, intranet and network resources, learning platform, software, handheld devices, equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will ensure any laptops and iPads I use have a password and will not reveal my password(s) to anyone.
- I will ensure that when I leave a work area, laptops or iPads will be locked to prevent a data breach.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality policy.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, school email system for any school business (currently: g-mail) and relevant communication with parents/carers regarding appropriate school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network/ Internet that does not have up-to-date anti-virus software.
- I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.
- I will not use personal digital cameras or any device with camera capabilities for taking and transferring images of pupils or staff without permission.
- I will not use school equipment to charge personal devices.
- I will ensure that any private social networking sites that I create or actively contribute to are not confused with or associated with my professional role or the school.
- I will ensure that all social media sites are set to private, so only my 'friends' can view information.
- I will ensure any confidential data that I wish to transport is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I will embed/ support the school's e-safety curriculum into my teaching.
- I understand that all Internet usage/ and network usage can be logged and this information could be made available to my manager on request.
- I understand that failure to comply with this agreement could lead to disciplinary action.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.

I agree to abide by all the points above.

Signature: _____ Date: September 2018

Full Name: _____ (printed)

Job title: _____

APPENDIX 4

St Anne's Catholic Primary School
Loving & learning together in Harmony with Christ

KS1 Acceptable Use Policy

- I will use the school's ICT equipment and tools (including computers, cameras etc.) for schoolwork and homework. If I need to use the school's computers for anything else, I will ask for permission first.
- I will only use the internet and email when an adult is nearby.
- I will not share my passwords with other people and will tell my teacher if I think someone else knows them.
- I will ask an adult before opening an email from someone I don't know.
- I will not share details about myself such as surname, phone number or home address.
- I will ask if I need to look at other peoples' work on the computer.
- I will ask my teacher before using photos or video.
- If I see something on a screen which upsets me, I will always tell an adult.

I will do my best to follow these rules because I know they are there to keep me and my friends safe.

If I don't follow these rules, I know that my teacher may stop me using technology at school and talk to my parent/guardian about how I use technology.

PLEASE RETURN TO CLASS TEACHER.

…….. (child's name) has discussed and agreed to follow the E-Safety rules, to support the safe use of ICT at St Anne's Catholic Primary School.

Parent/Guardian Signature: _____

Child's signature: _____ Year: _____ Date: _____

APPENDIX 5

St Anne's Catholic Primary School
Loving & learning together in Harmony with Christ

KS2 Acceptable Use Policy

- I will use the school's ICT equipment and tools for schoolwork and homework. If I need to use the school's computers for anything else, I will ask for permission first.
- I will only use the Internet if a teacher or teaching assistant is in the room with me.
- I will only delete my own files unless my teacher gives me permission to delete someone else's. I will not look at other people's files without their permission.
- I will keep my passwords private and tell an adult if I think someone else knows them.
- I will only open e-mail attachments from people who I know or an adult has approved. If I am unsure about an attachment or e-mail, I will ask an adult for help.
- I will not give my own personal details such as surname, phone number or home address or any other personal details that could be used to identify me, my friends or my family. If I have to use an online name I will make one up!
- I will never post photographs or video clips of people I know without permission and never include names with photographs or videos.
- I will never arrange to meet someone I have only ever previously met online. It could be dangerous.

I will do my best to follow these rules because I know they are there to keep me and my friends safe.

If I don't follow these rules, my teacher may:

- Speak to me about my behaviour.
- Speak to my parent/ guardian about my use of technology.
- Remove me from online communities or groups.
- Turn off my access for a little while.
- Not allow me access to use laptops / computers to access the internet or particular programmes.
- Take other action to keep me (and others) safe.

PLEASE RETURN TO CLASS TEACHER.

_____ (child's name) has discussed and agreed to follow the E-Safety rules, to support the safe use of ICT at St Anne's Catholic Primary School.

Parent/Guardian Signature: _____

Child's signature: _____ Year: _____ Date: _____

Appendix 6:

St Anne's Catholic Primary School
Loving & learning together in Harmony with Christ

Year 6 Mobile Phone Permission Form

The use of mobile phones in school is strongly discouraged. **The school cannot take responsibility for loss or damage to phones.**

It is recognised that some pupils do require mobile phones for their journeys to and from school. Under these circumstances mobile phones may be switched on and used outside normal school hours.

Mobile phones will be handed to the class teacher at the beginning of the day, and stored in a lockable area. Children will receive their mobile phones at the end of the day, or when they go home. If a phone is activated during school hours, without the permission of a member of staff, it will be confiscated for the rest of that school day. If the mobile phone is used inappropriately, i.e. taking photographs or videos without permission, this privilege will be removed.

Parent/Guardian Permission

I have read and understand the above information about appropriate use of mobile phones at St Anne's Catholic Primary School. I understand that this form will be kept on file at the school and that the details may be used (and shared with a third party) to assist in the identification of a phone should the need arise (e.g. if lost, or if the phone is being used inappropriately).

I give my child permission to carry a mobile phone to school and understand that my child will be responsible for ensuring that the mobile phone is used appropriately and correctly.

I understand that the school accepts no responsibility for pupils who lose or have their mobile phones stolen.

Parent name (print): _____

Parent signature: _____

Date: _____

Pupil name (print): _____

Mobile phone number: _____

Pupil signature: _____

Date: _____