Great Aycliffe
Catholic Schools'
Federation

Mission Statement

We believe that each person is unique and created in God's image.

In our federation, we provide a distinctive Catholic education, where each child is loved, nurtured, inspired and challenged to aspire to excellence and develop their individual abilities for themselves and others

E-Safety Policy

Including the Use of Photographic Devices and Recordings in School

Modified with grateful permission from Kent County Council

1. **<u>Who will write and review the policy?</u>**
   - The school has appointed an e–Safety Coordinator; this is the named person for Child Protection.
   - The e–Safety Policy and its implementation will be reviewed annually.
   - Our e–Safety Policy has been written by the school, building on the DCC e–Safety Policy and government guidance.
   - Our School Policy has been agreed by the Staff and approved by governors
   - Our school has formed an e-safety committee: the School Council and a parent governor.
   - The School has appointed a member of the Governing Body to take lead responsibility for e-Safety.

2. **<u>Teaching and learning</u>**

2.1. Why is Internet use important?

- Internet use is part of the statutory curriculum and is a necessary tool for learning.
- The Internet is a part of everyday life for education, business and social interaction.
- The school has a duty to provide students with quality Internet access as part of their learning experience.
- 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 students who show a responsible and mature approach to its use.

2.2. How does Internet use benefit education?

- 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 DCC and DfE;
- access to learning wherever and whenever convenient.

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

2.4. How will pupils learn how to evaluate Internet content?

- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught to use search engines appropriately for their age.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

3. Managing Information Systems

3.1. How will information systems security be maintained?

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- The school will comply with the terms of the data protection act, and is responsible for registering with the information commissioner's office. www.ico.gov.uk advice is available from www.ico.gov.uk/for_organisations/sector_guides/education.aspx
- Personal data sent over the Internet or taken off site will be encrypted.
- Portable media may not be used without specific permission followed by an anti-virus / malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The ICT coordinator/network manager will review system capacity regularly.
- The use of user logins and passwords to access the school network will be enforced.

3.2. How will email be managed?

- Pupils may only use approved email accounts for school purposes.
- Pupils must immediately tell a designated member of staff if they receive an 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.
- Staff will only use official school provided email accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Team. This may be via the school email account (stjosephsnewtonaycliffe@durhamlearning.net).
- All school e-mails must end with a disclaimer as distributed by the Head Teacher.
- The e-mail addresses of parents should not be shared with others. E-mails to multiple recipients which include parents should have the e-mail addresses **Blind Carbon Copied** (bcc).
- 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 would be.
- The forwarding of chain messages is not permitted.
- Staff should not use personal email accounts during school hours or for professional purposes.

3.3. How will published content be managed?

- 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 photos will only be published if consent has been given.
- The Head Teacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

3.4. Can pupils' images or work be published?

- Images or videos that include pupils will be selected carefully and will not provide material that could be reused.

- Pupils’ full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before images/videos of pupils are electronically published.
- Pupils’ work can only be published with their permission.
- Written consent will be kept by the school whilst pupils remain in school.
- The School will have a policy regarding the use of photographic images of children which outlines policies and procedures.(See appendix 2)

3.5. How will social networking, social media and personal publishing be managed?

- The school will control access to social media and social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name; address; mobile or landline phone numbers; school attended; IM (Instant Message); email addresses; full names of friends/family; specific interests and clubs etc.
- Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the Senior Leadership Team before using Social Media tools in the classroom.
- Staff official blogs or wikis should be password protected and run from the school website with approval from the Senior Leadership Team. Members of staff are advised not to run social network spaces for pupil use on a personal basis.
- Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Concerns regarding students’ use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students’ underage use of sites.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Policy.

3.6. How will filtering be managed?

- YouTube is accessible in school, but staff are required to ensure that video footage is downloaded first and checked rather than played live from the site.
- The school’s broadband access will include filtering.
- The school will have a system in place to make changes to the filter, including deciding who is responsible for authorising changes.
- Websites which schools believe should be blocked centrally should be reported to the ICT Service Desk. Teachers should always evaluate any websites/search engines before using them with their students; this includes websites shown in class as well as websites accessed directly by the pupils. Often this will mean checking the websites, search results etc., just before the lesson. Remember that a site considered safe one day may be changed due to the Internet being a dynamic entity. Particular attention should also be paid to advertisements as they can change each time the web page is accessed.
- The ICT Service Desk can alter the filter to school if the Head Teacher or Deputy Head Teacher contacts them with their PIN number.
- The school will work with DCC to review filtering.

- The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure.
- If staff or pupils discover unsuitable sites, the URL will be reported to the School e-Safety Coordinator who will then record the incident and escalate the concern as appropriate. The HT will report it to ICT Service Desk as above and complete the Log of Unsuitable Websites (Appendix 1).
- The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team.
- The School Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Durham Police or The Child Exploitation and Online Protection Centre (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.

3.7. How will videoconferencing be managed?

- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- Videoconferencing contact information will not be put on the school Website.
- The equipment must be secure and if necessary locked away when not in use.
- School videoconferencing equipment will not be taken off school premises without permission.
- Responsibility for the use of the videoconferencing equipment outside school time will be established with care.

Users

- Pupils will ask permission from a teacher before making or answering a videoconference call.
- Videoconferencing will be supervised appropriately for the pupils' age and ability.
- Parents' and carers' consent should be obtained prior to children taking part in videoconferences.
- 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 videoconference 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.
- Videoconferencing 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 videoconference. If it is a non-school site it is important to check that they are delivering material that is appropriate for your class.

3.8. How are emerging technologies managed?

- 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 in accordance with the school Acceptable Use or Mobile Phone Policy.

3.9. How should personal data be protected?

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

4. Policy Decisions

4.1. How will Internet access be authorised?

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- All staff will read and sign the School Acceptable Use Policy before using any school ICT resources.
- Parents will be asked to read the School Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.
- All visitors to the school site who require access to the schools network or internet access will be asked to read and sign an Acceptable Use Policy.
- Parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability.
- At EYFS / Key Stage 1 pupils' access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials.
- At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary.

4.2. How will risks be assessed?

- 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 Durham CC can accept liability for the material accessed, or any consequences resulting from Internet use.
- The school 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 and breaches will be reported to Durham Police.
- Methods to identify, assess and minimise risks will be reviewed regularly.

4.3. How will the school respond to any incidents of concern?

- All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc).
- The e-Safety Coordinator will record all reported incidents and actions taken in the Bullying or Child protection log.
- The Designated Child Protection Coordinator will escalate any e-Safety incidents 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 any 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 or e-Safety officer 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 County 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 school in Durham.

4.4. How will e–Safety complaints be handled?

- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- Any complaint about staff misuse will be referred to the head teacher.
- All e–Safety complaints and incidents will be recorded by the school, including any actions taken.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with the school to resolve issues.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- Discussions will be held with the local Police Safer Schools Partnership Coordinators and/or Children's Safeguard Team to establish procedures for handling potentially illegal issues.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to themselves or any other members of the school community.

4.5. How is the Internet used across the community?

- The school will liaise with local organisations to establish a common approach to e–Safety.
- The school will be sensitive to Internet-related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.
- The school will provide appropriate levels of supervision for students who use the internet and technology whilst on the school site.
- The school will provide an Acceptable Use Policy (AUP) for any guest who needs to access the school computer system or internet on site.

4.6. How will Cyberbullying be managed?

- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.
- Support would be put in place for anyone in the school community affected by cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of Cyberbullying.
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.
- Sanctions for those involved in cyberbullying may include:
  - The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
  - Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools Anti-Bullying Policy.
  - Parent/carers of pupils will be informed.
  - The Police will be contacted if a criminal offence is suspected.

4.7. How will Learning Platforms (LPs) be managed?

- SLT and staff will regularly monitor the usage of the LP by pupils and staff in all areas, in particular message and communication tools and publishing facilities. (This is the DLG at St. Joseph's.)
- Pupils/staff will be advised about acceptable conduct and use when using the DLG.
- Only members of the current pupil, parent/carers and staff community will have access to the DLG.
- All users will be mindful of copyright issues and will only upload appropriate content onto the DLG.
- When staff, pupils etc. leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.
- Any concerns about content on the DLG may be recorded and dealt with in the following ways:
  a) The user will be asked to remove any material deemed to be inappropriate or offensive.
  b) The material will be removed by the site administrator if the user does not comply.
  c) Access to the DLG for the user may be suspended.
  d) The user will need to discuss the issues with a member of SLT before reinstatement.
  e) A pupil's parent/carer may be informed.

- A visitor may be invited onto the DLG by a member of the SLT. In this instance there may be an agreed focus or a limited time slot.
- Pupils may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.

4.8. How will mobile phones and personal devices be managed?

- Mobile phones and personal devices will not be used during lessons or formal school time. They should be switched off/turned to silent at all times unless permission has been given by a member of Senior Leadership Team in emergency circumstances.
- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum based activity with consent from a member of staff.
- The Bluetooth function of a mobile phone/iPad should be switched off at all times and not be used to send images or files to other mobile phones.
- 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 are not permitted to bring to school mobile devices. If a pupil breaches the school policy then the phone will be confiscated and will be held in a secure place in the school office.
- A school mobile phone is available.
- Staff should not use personal devices such as mobile phones or cameras to take photos.
- 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. Contact may be required whilst on a school trip. This should be done through the school emergency contact numbers.
- Videos of pupils and will only use work-provided equipment for this purpose. If a member of staff has permission granted by the HT to use their own camera, it must be solely for school use and have its memory cleared at least monthly.
- If a member of staff breaches the school policy then disciplinary action may be taken.

5. Communication Policy

5.1. How will the policy be introduced to pupils?

- All users will be informed that network and Internet use will be monitored.

- An e–Safety training programme will be established across the school to raise the awareness and importance of safe and responsible internet use amongst pupils.
- E-Safety rules or copies of the student Acceptable Use Policy will be posted in classrooms.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.

5.2. How will the policy be discussed with 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 will implement Acceptable Use Policies.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is 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.
- The School will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the pupils.
- 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.

5.3. How will parents' support be enlisted?

- Parents' attention will be drawn to the school e–Safety Policy in newsletters and on the school website.
- Parents will be requested to sign an e–Safety/Internet agreement as part of the Home School Agreement.
- Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss its implications with their children.
- Information and guidance for parents on e–Safety will be made available to parents in a variety of formats.
- Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parents.

Please read this policy with reference to the Equal Opportunities Policy, the Special Educational Needs Policy, the Disability Equality Scheme and the Health and Safety Policy. The Policy on the Use of Photographic Devices and Recordings in School is included in Appendix 2. The governing body will comply with relevant legislation. They will promote equality in race gender and disability (in accordance with Diocesan guidance).

Review date: Autumn 2015
Approved by governors in ____ 2014

Appendix 1 Log of Unsuitable Website Form

Appendix 2 Policy on the Use of Photographic Devices and Recordings in School

Appendix 3 Pupils e-safety agreement KS2

Appendix 4 Pupils e-safety agreement KS1/FS

Appendix 5 Adult acceptable use policy

Appendix 6 E-Safety Contacts and References

Appendix 1 Log of Unsuitable Websites

Date of email	staff reporting	website address	concern	date reported to ICT Services	outcome

Appendix 2

Great Aycliffe Catholic Schools' Federation

Great Aycliffe Catholic School Federation

Policy on the Use of Photographic Devices and Recordings in School

Introduction

The governors and staff of the Great Aycliffe Catholic Schools' Federation are aware that there is a possibility that photographic images can be used inappropriately and/or for illegal purposes.

It is also understood that families like to record events in their child's school career.

Photographs or other recordings generated by parents at a school event are for the sole use of the family concerned. They are not for display, distribution or any other purpose outside of that family. Photographs or other recordings generated by staff or by a third party on behalf of either school at a school event are for the sole use of the school and the families within it. Photographs, with consent, may be e-mailed to a newspaper.

Rationale

The Governing Body wishes to make every effort to prevent any inappropriate use of photographic or recorded images of pupils in the Great Aycliffe Catholic Schools' Federation, whilst acknowledging that families may wish to photograph or record their children at school events throughout their school career.

Aims

- To protect pupils, families and staff from inappropriate use of photographic images.
- To comply with performance licence requirements/legislation.

Procedure

- Images of children and staff may be used in school brochures.
- Images of children and staff may be sent to a newspaper.
- All parents will be required to complete the attached consent form acknowledging the school statement. If a form is not returned, then parental consent is assumed.
- The consent form will be retained on the child's school records for the period he or she remains in school.
- All recordings are subject to the performance licence (if required) in place for the recording of a production.
- Before recordings are made by or on behalf of the school a letter will be sent to parents or guardians informing them of the school's intent and requesting specific consent.

Note

Parents need to understand that:

- Where they feel unable to agree to the statement limiting the taking and use of photographs or recordings, it may be necessary to prohibit the taking of photographs or recordings by that parent.
- Where parents feel unable to agree that the school and/or other parents, in accordance with this statement, should be permitted to take photographs or recordings of their child, it may be necessary to prohibit any parent from taking photographs or recordings.

Further guidance may be found in Durham County Council's *Guidance on the Use of Images of People: Photographs, Videos and Webcams*.

Consent Form

I acknowledge the federation's policy on the use of photographic devices and recordings and agree that any photographs or recordings that I produce are for the sole use of my family.

I consent / do not consent***** to my child being photographed or recorded during school activities by staff of the school and by parents of other children who attend the school, or a third party hired for this specific purpose, in accordance with the federation policy.

I consent / do not consent ***** to my child being photographed for the school brochure.

I consent / do not consent ***** to my child being photographed and the photographs being e-mailed or sent to a newspaper.

I consent / do not consent ***** to my child being photographed for the school and/or federation website.

I will honour the performance licence in place for the recording of a production.

I understand that this consent form will be retained by the school on my child's file until he or she leaves the school.

Signed ____________________________________

Parent / guardian of ____________________________________

Date ____________________________________

If a form is not returned, or is returned blank, then parental / guardian consent will be assumed.

***** please delete as appropriate

Great Aycliffe Catholic School Federation

Policy on the Use of Photographic Devices and Recordings in School

Consent Form for a Performance Recorded by School

Performance of ________________________________

on ________________________________ (date(s)

I acknowledge the federation’s policy on the Use of Photographic Devices and Recordings in School.

I consent/ do not consent***** to my child being photographed or recorded during the performance of the above by staff of the school, or by a third party on behalf of the school, in accordance with the federation policy.

I will honour the performance licence in place for the recording of a production.

I understand that this consent form is for the above performance only. It will be retained by the school on my child’s file until he or she leaves the school.

Signed ____________________________________

Parent / guardian of ____________________________________

Date ____________________________________

If a form is not returned, or is returned blank, then parental / guardian consent will be assumed.

***** please delete as appropriate

Great Aycliffe Catholic School Federation

Policy on the Use of Photographic Devices and Recordings in School

Staff Consent Form

I acknowledge the federation’s policy on the use of photographic devices and recordings and agree that any photographs or recordings that I produce are for the sole use of me, the federation and my family.

I consent/ do not consent***** to being photographed or recorded during school activities by other staff of the school and by parents of children who attend the school, or a third party hired for the specific event, in accordance with the federation policy.

I consent / do not consent ***** to being photographed for the school brochure.

I consent / do not consent ***** to being photographed and the photographs being e-mailed or sent to a newspaper.

I consent / do not consent ***** to being photographed for the school and/or federation website.

I will honour the performance licence in place for the recording of a production.

I understand that this consent form will be retained by the school on my file until I leave the school.

Signed ____________________________________

Print Name ____________________________________

Date ____________________________________

If a form is not returned, or is returned blank, then parental / guardian consent will be assumed.

***** please delete as appropriate

Appendix 3

Great Aycliffe Catholic Schools' Federation

St. Mary's R.C. (V.A.) Primary School

Newton Aycliffe

Pupils' e-safety agreement KS2

For my own personal safety – everywhere!

- I will ask permission from a member of staff before using the Internet at school
- I am aware of "stranger danger" when on line and will not meet online friends
- I will tell an adult about anything online which makes me feel uncomfortable
- I will not try to bypass the system to reach websites the school has blocked
- I understand that the school may check my files and may monitor the web pages I visit
- When in school I will only contact people with my teachers permission

- I will be very careful when sharing pictures or video of myself or my friends, if I am in school I will always check with a teacher
- I will not put my "Personal Information" online. (My full name, birthday, phone number, address, postcode, school etc.)

To keep the system safe

- I will only use my own login and password, which I will keep secret
- I will not access other people's files
- I will not play games on a school computer unless my teacher has given me permission
- I will not install software on school computers
- I will not use the system for gaming, gambling, shopping, or uploading videos or music

Responsibility to others

- The messages I send will be polite and responsible
- I will not upload images or video of other people without their permission
- Where work is copyrighted (Including music, videos and images) I will not either download or share with others.
- I understand that the school may take action against me if I am involved in incidents of inappropriate behaviour wherever their location. If the activities are illegal this may be reported to the police.

Personal Devices

- The school cannot accept responsibility for loss or damage to personal devices
- It is not permitted for pupils to bring mobile phones to school.
- Other devices (e.g. Games consoles, cameras) should only be brought into school with permission from a teacher.

Pupils e-safety contract

Please complete, sign and return to the school secretary

Pupil:	***Form:***

Pupil's Agreement

I have read and I understand the pupils e-safety agreement, and will abide by the rules which are designed to keep both myself and the school safe

Signed:	***Date:***

Parent's Consent

I have read and understood the e-safety agreement and give permission for my son / daughter to access the Internet at school, and will encourage them to abide by these rules. Children will receive advice on e-safety at school. Advice for parents is available at www.thinkuknow.org.uk/parents or by contacting the school. I understand that the school will take reasonable precautions to ensure pupils cannot access inappropriate materials. I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

I will ensure that any pictures taken during school events that include other children will not be shared using social media.

Signed:	***Date:***

Please print name:

Appendix 4

Great Aycliffe Catholic Schools' Federation

St. Mary's R.C. (V.A.) Primary School
Newton Aycliffe

Pupils' e-safety agreement FS/KS1

Keeping me safe at home and at school

We check with a grown up before using the internet

We tell a grown up if something we see makes us feel worried

If we get stuck or lost on the internet we will ask for help.

We can write polite and friendly **messages** to people we know

We will keep our personal information, our name, address, our school, our pictures "Top Secret" and not share it on the internet.

We will not bring mobile phones to school

Pupils e-safety contract

Please complete, sign and return to the school secretary

Pupil:	***Form:***

Pupil’s Agreement

I have read and I understand the pupils e-safety agreement, and will abide by the rules which are designed to keep both myself and the school safe

Signed:	***Date:***

Parent’s Consent

I have read and understood the e-safety agreement and give permission for my son / daughter to access the Internet at school, and will encourage them to abide by these rules. Children will receive advice on e-safety at school. Advice for parents is available at www.thinkuknow.org.uk/parents or by contacting the school. I understand that the school will take reasonable precautions to ensure pupils cannot access inappropriate materials. I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child’s e-safety.

I will ensure that any pictures taken during school events that include other children will not be shared using social media.

Signed:	***Date:***

Please print name:

Great Aycliffe
Catholic Schools'
Federation

Appendix 5
St. Mary's R.C. (V.A.) Primary School
Newton Aycliffe

Adult ICT Acceptable Use Policy 2014

As a professional organisation with responsibility for children's safeguarding it is important that all staff (including supply and agency staff; those on work placement and volunteers) take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

- I understand that Information Systems and ICT include networks, data and data storage, online, offline communication technologies, and access devices. Examples include mobile phones, PDAs, digital cameras, email and social media sites**.**
- Mobile phones must not be used during lesson times.
- Contact may be required with parents whilst on a school trip. This should be done through the school emergency contact numbers. A school mobile phone is available.
- School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
- I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.
- I will respect system security and I will not disclose any password or security information. I will use a 'strong' password, as required by the school network system.
- I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.
- I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1988. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls) or accessed remotely. Any data which is being removed from the school site via memory sticks and laptops will be encrypted by a method approved by the school. Data sent via e-mail on the Durham Learning Gateway (DLG) is protected. If DLG e-mail is accessed on personal devices such as Smart phones, iPads, tablets and other similar devices this should only be accessed by staff and devices secured with passwords or passkeys. Any

images or videos of pupils will only be transported by secure media and will always take into account parental consent.

- I will not keep professional documents which contain school-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are secured and encrypted and I have received written permission from the HT. Where possible I will use the School Learning Platform (DLG) to upload any work documents and files in a password protected environment. I will protect the devices in my care from unapproved access or theft.
- I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.
- I will respect copyright and intellectual property rights.
- I have read and understood the school e-Safety policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.
- I will report all incidents of concern regarding children's online safety to the Designated Child Protection Coordinator / the e-Safety Coordinator (the Head Teacher) as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the e-Safety Coordinator or the designated lead for filtering as soon as possible.
- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any school related documents or files, then I will report this to the ICT Support Provider/Team (ITSS or the HT) as soon as possible.
- My electronic communications with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number. Any pre-existing relationships which may compromise this will be discussed with the Senior Leadership team.
- My use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with the school AUP and the Law.
- I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the County Council, into disrepute. This would include any comment made, even in the belief that it is private on a social media site.
- I will promote e-Safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.
- If I have any queries or questions regarding safe and professional practice online, either in school or off site, then I will raise them with the Head Teacher.
- I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

The School may exercise its right to monitor the use of ~~i~~nformation systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood and agree to comply with the Staff ICT Acceptable Use Policy.

Signed: ……………………….... Print Name: ……………………. Date: ………

Accepted by: …………………………… Print Name: …………………………

Appendix 6

E-Safety Contacts and References

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

Childline: www.childline.org.uk

Childnet: www.childnet.com

Click Clever Click Safe Campaign: http://clickcleverclicksafe.direct.gov.uk

Cybermentors: www.cybermentors.org.uk

Digizen: www.digizen.org.uk

Durham EDS – E-safety, Teaching and learning advice Tel: 0191 3834370

Durham Safeguarding Children Board (DLSCB): www.durham-lscb.gov.uk

ICT Service Desk – Changes to filtering Tel: 03000 261100

ICTSS Service Desk – All other ICT issues Tel: 01388 424999

Internet Watch Foundation (IWF): www.iwf.org.uk

Kent e–Safety in Schools Guidance: www.kenttrustweb.org.uk?esafety

Kidsmart: www.kidsmart.org.uk

Schools e–Safety Blog: www.kenttrustweb.org.uk?esafetyblog

Teach Today: http://en.teachtoday.eu

Think U Know website: www.thinkuknow.co.uk

Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com