St Nicholas Primary School

E-Safety (On-line Safety) Policy

Last reviewed Spring 2017

This policy should be read in conjunction with the following policies:

Behaviour, Inclusion, Health & Safety, Data Protection and Curriculum

Reviewed by: Ms S Middleton

Date Approved by the Governing Body: 20 March 2017

Minute Number: TBA

Date of Next Review: Spring 2018 or as required

St Nicholas Primary School

CONTENTS

SECTION		PAGE NUMBER
1.	Introduction - E-safety	3
2.	End to End E-Safety	3
3.	Learning & Teaching	3
4.	Staff Training	4
5.	Managing ICT Systems and Access	5
6.	E-mail	6
7.	Social Networking	6
8.	Pupils Publishing Content Online	7
9.	Managing & Filtering	7
10.	Managing Emerging Technologies	8
11.	Mobile Phones and Devices	8
11.1	General Use of Personal Devices	8
11.2	Pupils' Use of Personal Devices	8
11.3	Staffs' Use of Personal Devices	9
12.	CCTV	9
13.	Authorising Internet access	9
14.	Data Protection and Information Security	9
15.	Management of Assets	10
16.	Enlisting Parents' support	10
17.	Response to an Incident of Concern	11
Appendix 1	Response to Risk Flowchart	12
Appendix 2	E-safety Incident Sheet	13
Appendix 3	Outcome	14
Appendix 4	KS2 Pupil Online Digital Agreement	15
Appendix 5	Early Years and KS1 - Pupil Internet Agreement	16
Appendix 6	Rules for Responsible Internet Use	17
Appendix 7	On-Line Safety Audit	18

St Nicholas Primary School

1. Introduction - E-Safety

- E-Safety encompasses the use of new technologies, internet and electronic communications such as mobile phones, games consoles, tablets and PCs, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguarding and awareness for users to enable them to control their online experience.
- E-Security refers to the protection of data against the deliberate or accidental access by unauthorized persons and also includes protection against accidental damage or loss.

The school's e-safety policy will operate in conjunction with other policies including the Behaviour policy, Inclusion policy, Curriculum, Health and Safety and Data Protection.

2. End to End E-Safety

Online safeguarding depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of e-safeguarding policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from Kingston communications
- Effective management of filtering through the Netpilot system.

3. Learning and Teaching

We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We know that the internet and other technologies are embedded in our pupils' lives, not just in school but outside as well, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the internet brings.

- We will provide an ICT curriculum/PSHCE curriculum/other lessons which have e-safety related lessons embedded throughout
- We will celebrate and promote e-safety throughout the curriculum on a continuous basis rather than one off sessions. We will have a planned programme of assemblies and whole-school activities, including promoting Safer Internet Day each year.

- We will discuss, remind or raise relevant e-safety messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials.
- Any internet use will be carefully planned to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas.
- Pupils will be taught how to use a range of age-appropriate online tools in a safe and effective way.
- We will remind pupils and parents about their responsibilities when using the internet through an Acceptable Use Policy which every pupil/parent will sign (child responsibility document/Parent responsibility document).
- Staff will model safe and responsible behaviour in their own use of technology during lessons.
- We will teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area. Whilst doing this all pupils will use age appropriate search engines, all of which will be monitored and children taught about what to do if they come across something inappropriate.
- Pupils will be taught about the impact of cyberbullying and know how to seek help if they are affected by any form of online bullying.
- Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline.

4. Staff training

From March 2017 our staff will receive annual training on e-safety issues with updates as and when new issues arise in the form of insets.

- As part of the induction process all new staff receive information and guidance on the e-safety policy, the school's Acceptable Use Policies, e-security and reporting procedures.
- All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community.
- All staff will be encouraged to incorporate e-safety activities and awareness into all their curriculum areas, on a continuous basis to keep momentum on the issue.

5. Managing ICT Systems and Access

- The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible
- Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.
- Servers, workstations and other hardware and software will be kept updated as appropriate.
- Virus protection is installed on all appropriate hardware, and will be kept active and up to date.
- Monitoring software is in place on the network on computers and laptops for both staff and children. This is reviewed by Alan Clark (ICT Technician) and Sarah Middleton (ICT Co-Ordinator). Activity reports are kept each term.
- Visual monitoring is done in class whilst children are on the I pads as monitoring software is not available for I pad devices.
- The school will agree which users should and should not have internet access and the appropriate level of access and supervision they should receive.
- All users will sign an end-user Acceptable Use Policy provided by the school, appropriate to their age and type of access. Users will be made aware that they must take responsibility for their use and behaviour while using the school ICT systems and that such activity will be monitored and checked.
- At Key Stage 1, pupils will access the network using an individual username (their first name) and a generic password, which the teacher visually supervises. All internet access will be undertaken alongside a member of staff or, if working independently, a member of staff will supervise at all times. It is the responsibility of the staff member involved to ensure children are logged out correctly.
- At Key Stage 2, pupils will have an individual user name with a generic password which will be kept secure, in line with the pupil Acceptable Use Policy. They will ensure they log out after each session and that no other pupil uses their log in details.
- Members of staff will log onto computer devices using an individual id and password, which they will keep secure. They will ensure that they log out after each session and not allow pupils to access the internet through their id and password. They will abide by the school AUP at all times. They will be aware that they have certain internet restrictions and their actions can be monitored.

6. E-mail

- Staff should not use personal email accounts during school hours or for professional purposes, especially to exchange any school-related information or documents.
- Staff and pupils should only use approved email accounts allocated to them by the school and should be aware that any use of the school email system will be monitored and checked
- Staff will be allocated an e-mail account for use in school.
- Pupils and staff are prohibited from using their personal email at school especially to exchange any school related documentation.
- Staff will only use official school-provided email accounts to communicate with pupils and parents and carers. Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- Staff who send emails to external organisations, parents or pupils, are advised to carbon copy (cc) the head teacher, line manager or another suitable member of staff into the email
- Pupils must immediately tell a teacher or trusted adult if they receive any inappropriate or offensive email.
- Irrespective of how pupils or staff access their school email (from home or within school), school policies still apply.
- Chain messages will not be permitted or forwarded on to other school-owned email addresses

7. Social Networking

- Staff will not post inappropriate content or participate in any conversations which will be damaging to the school.
- Staff who hold an account should not have pupils as their ‘friends’ under any circumstance.
- Staff friendship with parents is actively discouraged however will be assessed on an individual basis (ie: previous friendship before children joining the school)
- Any inappropriate friendship on social media can result in disciplinary action of the staff member.
- School blogs/podcasts or social media sites should be password protected and run from the school website with approval from the Senior Leadership Team/Senior manager.

8. Pupils Publishing Content Online

- Pupils will not be allowed to post or create content on sites unless the site has been approved by the school ie: Digitull.
- Teachers will model safe and responsible behaviour in their creation and publishing of online content within the school learning platform. For example, pupils will be reminded not to reveal personal information which may allow someone to identify and locate them.
- The copyright of all material will be held by the school, or be attributed to the owner where permission to reproduce has been obtained.
- Pupils full names will not be used anywhere on the website/blog, particularly in association with photographs and video.
- Written permission is obtained from parents/carers for every new admission and then annually for children before photographs and videos are taken/published.
- Any images, videos or sound clips of pupils must be stored on the school network and never transferred to personally-owned equipment
- The school will store images of pupils that have left the school for 2 years following their departure for use in school activities and promotional resources
- The E safety officer/technician is responsible for deleting images off the network when they are no longer required or the pupils have left the school.

9. Managing Filtering

- The school has the Netpilot filtering system in place which is managed by the schools ICT Technician.
- The school will have a clearly defined procedure for reporting breaches of filtering. All staff and pupils will be aware of this procedure by reading and signing the Acceptable Use Policy and by attending the appropriate awareness training.
- If staff or pupils discover an unsuitable site, it must be reported to the ICT Co-ordinator or a member of SLT immediately.
- If users discover a website with potentially illegal content, this should be reported immediately to the ICT Coordinator/SLT. The school will report such incidents to appropriate agencies including the ISP, Police, CEOP or the IWF
- Any amendments to the school filtering policy or block-and-allow lists will be checked and assessed by the Headteacher/ICT Co-ordinator prior to being released or blocked.
- The evaluation of online content materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

10. Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in the school is allowed.
- Emerging technologies can be software or hardware
- 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 the appropriate authorities

11. Mobile Phones and Devices

11.1 General use of personal devices

- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time.
- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- No images or videos will be taken on mobile phones or personally-owned devices. In the case of school productions, Parents/carers are permitted to take photographs of their own child in accordance with school protocols which strongly advise against the publication of any such photographs on Social networking sites.
- The school has 1 mobile phone which is to be used when on school trips for communication/emergencies, in some cases personal mobiles may need to be used.
- The sending of abusive or inappropriate text, picture or video message is forbidden.

11.2 Pupils' use of personal devices

- Children's mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off and handed into the school office at the beginning of the day and collected at the end of the day.
- If a pupil needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Pupils will be provided with school laptops/I pads to use in specific learning activities under the supervision of a member of staff, no home devices are allowed to be used within school.

11.3 Staffs' use of personal devices

- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families whilst inside school, however in the case of an emergency whilst **outside** of the school setting (ie on a school trip) it may be necessary to use your personal mobile to contact a **parent/carer only**.
- Staff will not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken
- 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 devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- The above is with exception to the caretaker who uses a personal mobile phone to arrange contractors, photograph health and safety issues on site.

12. CCTV*:*

- The school may use CCTV in some areas of school property as a security measures.
- Cameras will only be used in appropriate areas and there will be/is clear signage indicating where it is in operation.

13. Authorising Internet access

- All staff must read and sign the 'Acceptable Use Policy' before using any of school ICT resources.
- All parents will be required to sign the home-school agreement prior to their children being granted internet access within school
- All visitors and students will be asked to read and sign the Acceptable use policy prior to being given internet access within the school, they will then be given access to a separate guest wifi server.
- The school will maintain a current record of all staff, visitors and pupils who have
  granted access to the school's internet provision.

14. Data Protection and Information security

- The school community will act and carry out its duty of care for the information assets it holds in line with its Data Protection Act 1998/Data protection law 2015 commitments
- Any access to personal and sensitive information should be assessed and granted by the SIRO and the applicable IAO.

- All computers that are used to access sensitive information should be locked (Ctrl,Atl-Del) when unattended
- All access to the school information management system will be on a need-to-know or least privilege basis. All access should be granted through the SIRO or IAO
- All information on school servers shall be accessed through a controlled mechanism, with file permissions allocated and assessed on a need to know/ least privilege basis. All access should be granted through the SIRO or IAO
- Staff and pupils will not leave personal and sensitive printed documents on printers within public areas of the school
- All personal and sensitive information taken offsite will be secured through appropriate technical controls, e.g. encrypted USB sticks.
- All teachers have been issued with an encrypted USB stick to store and transport sensitive and personal information.
- All devices taken off site, e.g. laptops, tablets, removable media or phones, will be secured in accordance with the school's information-handling procedures and, for example, not left in cars or insecure locations
- Users should be vigilant when accessing sensitive or personal information on screen to ensure that no one else, who may be unauthorised, can read the information.

15. Management of Assets

- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- Disposal of any ICT equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007.
  Further information can be found on the Environment Agency website

16. Enlisting Parents' support

- Parents attention will be drawn to the school Online Safety policy and safety advice in newsletters, the school website and dedicated parent safety days.
- The school website will be used to provide parents with timely and meaningful information about their children's school lives and work to support the raising of achievement. The website will also provide links to appropriate online-safety websites.
- Termly parent support groups will be held for parents to 'drop' in and receive any advice they need or voice any concerns that they may have about their child in relation to online safety.

17. Response to an Incident of Concern

An important element of e-safeguarding is the ability to identify and deal with incidents of concern including the confidentiality of information. All staff/volunteers, children and young people have a responsibility to report online-safety or e-security incidents so that they may be dealt with effectively and in a timely manner in order to minimise any impact. The school has incident reporting procedures in place and from March 2017 we will record incidents in an "incident log". This log is securely locked away. The chain below demonstrates the key members of staff for which a cause for concern is dealt with in school.

Caroline Skipper -Head Teacher
Sarah Middleton – E-Safeguarding Officer

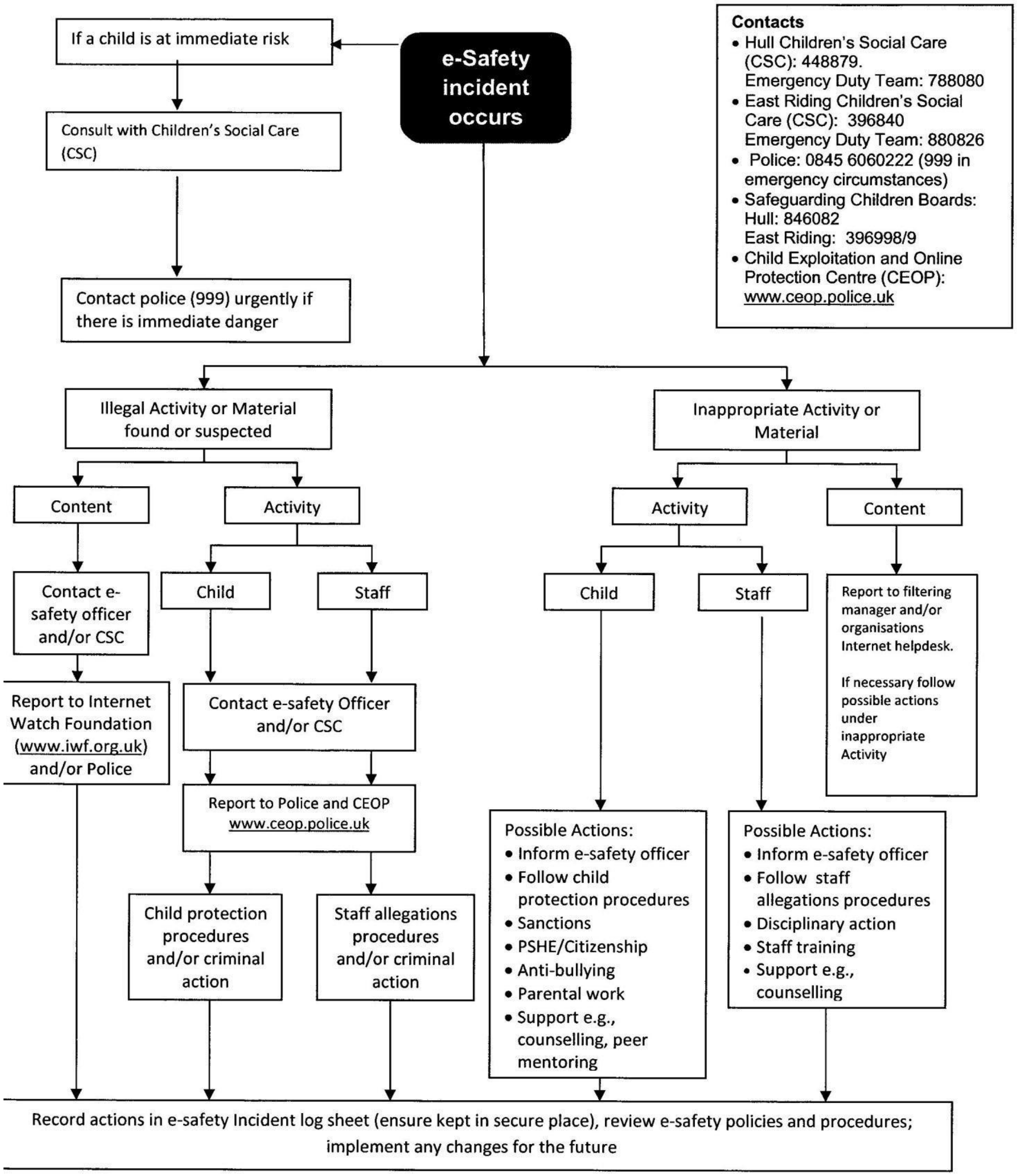
Helen Johnson and Sarah Collins – Safeguarding Officers

Sarah Leaf – Behaviour Co-ordinator

Appendix 1.

2.4.9 Response to Risk Flowchart

Response to and Reporting of an e-Safety Incident of Concern


e-Safety incident occurs
If a child is at immediate risk
Consult with Children's Social Care (CSC)
Contact police (999) urgently if there is immediate danger
Illegal Activity or Material found or suspected
Content
Activity
Contact e-safety officer and/or CSC
Report to Internet Watch Foundation (www.iwf.org.uk) and/or Police
Child
Staff
Contact e-safety Officer and/or CSC
Report to Police and CEOP www.ceop.police.uk
Child protection procedures and/or criminal action
Staff allegations procedures and/or criminal action
Inappropriate Activity or Material
Activity
Content
Child
Staff
Report to filtering manager and/or organisations Internet helpdesk.
If necessary follow possible actions under inappropriate Activity
Possible Actions:
• Inform e-safety officer
• Follow child protection procedures
• Sanctions
• PSHE/Citizenship
• Anti-bullying
• Parental work
• Support e.g., counselling, peer mentoring
Possible Actions:
• Inform e-safety officer
• Follow staff allegations procedures
• Disciplinary action
• Staff training
• Support e.g., counselling
Record actions in e-safety Incident log sheet (ensure kept in secure place), review e-safety policies and procedures; implement any changes for the future

Contacts

- Hull Children's Social Care (CSC): 448879.
  Emergency Duty Team: 788080
- East Riding Children's Social Care (CSC): 396840
  Emergency Duty Team: 880826
- Police: 0845 6060222 (999 in emergency circumstances)
- Safeguarding Children Boards:
  Hull: 846082
  East Riding: 396998/9
- Child Exploitation and Online Protection Centre (CEOP): www.ceop.police.uk

St Nicholas Primary School

Appendix 2.

E Safety Incident Sheet

Name of pupil:
Class:
Referred by:

Date of referral:
Time of referral:

Concern:

Action to be taken	✓	Date	Time
Referral to Headteacher- Caroline Skipper			
Referal to ICT Co-ordinator – Sarah Middleton			
Referal to CEOP			
Passed onto Police			
Parents informed by phone			
Parents asked in for a meeting			
Esafety Intervention sessions			

Area of concern	Please tick appropriate box
Cyberbullying	
Grooming	
Obscene/offensive messages	
Data Security	

Appendix 3.

Outcome:

St Nicholas Primary School

Appendix 4.

St Nicholas KS2 Pupil Online Digital Agreement

As part of pupil's curriculum enhancement and the development of ICT skills, St Nicholas Primary School is providing supervised access to the internet. Our internet access has a built-in filtering system that restricts access to sites containing inappropriate content. No system is perfect, however, and you should be aware that it is not possible to remove entirely the risk of finding unsuitable material.

ACTION

1. **Read this with your parent(s).**
2. **Sign it.**
3. **Supervised access will only be allowed after this is returned to school.**

- □ I will be responsible for my own behaviour on the Internet, just as anywhere else in school
- □ If I see something I am unhappy with or receive a message I do not like I will tell a member of staff immediately to protect myself and other pupils
- □ I will not try to find websites in school that are not to do with my work or which I know will be offensive, rude or unpleasant
- □ I understand that the school may check my computer files and may monitor the Internet sites I visit;
- □ I will not take part in any bullying using phones, messaging or other IT equipment and will tell if I know someone else in school is.
- □ I will not use any rude language when commenting on the website, in emails and on my learning space
- □ I will contact only people I know or those the teacher has approved.
- □ I will only use the internet with permission from a member of staff
- □ I will not access other people's files unless permission has been given.
- □ I will only use computers for schoolwork and homework unless permission has been granted otherwise
- □ I will not download any programs to the computer from the Internet and will not bring programs from home for use in school.
- □ I will not give out personal information such as full name, phone number and address and will tell an adult if anyone tries to make an arrangement to meet me
- □ If I choose not to follow these rules I understand I will not be allowed access to Internet resources and be in trouble for poor behaviour

I have read through this agreement with my child and agree to these safety restrictions.

Signed: …………………………….(Parent/Carer) Date ………………

Name of child: ……………………………………………. Class……………….

St Nicholas Primary School

Appendix 5.

St Nicholas Primary School Early Years and KS1 - Pupil Internet Agreement

As part of pupil's curriculum enhancement and development of ICT skills, St Nicholas is providing supervised access to the internet including emails.

Our internet access has a built in filtering system that restricts access to sites containing inappropriate content. No system is perfect, however, and you should be aware that it is not possible to remove entirely the risk of finding unsuitable material.

Action

- **Read this with your child,**
- **Sign it and return it to school.**

I agree I will:

□ Only use the Internet when an adult is with me or has given me permission

□ Tell my Teacher if anything makes me feel uncomfortable or unhappy on the Internet

□ Not give my personal details out to anyone who I don't know or who is not a friend in real life.

□ Make sure that if I send a message I will always be polite

□ Never take photos of others or upload them without my teachers permission

□ Not log into Internet games without asking my teacher first

Signed Parent/Carer ……………………………….. Date ………………..

Name of Child………………………....... Class…………………

Appendix 6.

St Nicholas Primary School

Rules for Responsible Internet Use

The school has installed computers and Internet access to help our learning. These rules will keep everyone safe and help us be fair to others.

- I will use only my own login and password which I will keep a secret
- I will not access other people's files.
- I will only use the school network for school work and homework.
- Any messages I send will be polite and sensible.
- I will not give my name, home address or phone number; or arrange to meet someone, unless this is part of an approved school project and with the support of an adult.
- I will not send photos or video of myself and other pupils unless this is part of an approved school project.
- To help protect other pupils and myself, I will tell a member of staff if I see anything I am unhappy with or I receive a message I do not like.
- I understand that the school can check my computer files and the Internet sites I visit.

The school has an online-safety Policy that complies with HCC guidance.	Y/N
Date of latest update:	
The Policy was agreed by governors on:	
The Policy is available for staff at	
And for parents/carers at	
The Designated teacher for Child Protection is	
The online-safety Officer is	
The responsible member of the governing body is	
Has online-safety training been provided for all children and all members of staff including governors?	
Is there a clear procedure for a response to an incident of concern?	
Are all staff/volunteers, children, parents /carers aware that network activity and internet use is closely monitored and can be traced?	
Is the Think U Know training being considered?	Y/N
All staff sign an Acceptable ICT Use Agreement on appointment.	Y/N
Parents sign and return an agreement that their child will comply with the school Acceptable ICT Use statement.	Y/N
Rules for Responsible Use have been set for students:	Y/N
These Rules are displayed in all rooms with computers.	Y/N
Internet access is provided by an approved educational Internet service provider and complies with DfES requirements for safe and secure access.	Y/N
The school filtering policy has been approved by SLT.	Y/N
An e-security audit has been initiated by SLT.	Y/N
School personal data is collected, stored and used according to the principles of the Data Protection Act.	Y/N
Staff with responsibility for managing filtering and network access monitoring work within a set of procedures and are supervised by a member of SLT.	Y/N

St Nicholas Primary School

Appendix 7. Online-safety Audit