-

We all shine like stars

Norton Church Of England Primary School

E- SAFETY POLICY

Doc:	E-Safety	Date Issued:	19/09/16
Version:	8	Agreed By Staff:	19/09/16
Category:	Policy	Agreed by Governors:	19/09/16
Comments:	This Policy is due review September 2017		

AMENDMENT HISTORY

Version	Date Issued	Originator/ Modified by	Reason(s) For Issue/ Re-issue
1	Sept 2009	Jane Johnson	New policy. Major extension from previous internet policy
2	Sept 2010	Jane Johnson	Review
3	Sept 2011	Jane Johnson Caroline Cundick	Review
4	Sept 2012	Jane Johnson	Review and update
5	Sept 2013	Jane Johnson	Review
6	Sept 2014	Jane Johnson	Review
7	Sept 2015	Jane Johnson	Review
8	Sept 2016	Jane Farren	Annual review with contact details updated

E- SAFETY POLICY

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The school's e-safety policy will operate in conjunction with other policies including those for Pupil Behaviour, Anti-Bullying, Child Protection, Curriculum, Data Protection and Security.

Good Habits

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the provider including the effective management of content filtering.
- National Education Network standards and specifications.

Dangers to consider

Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience towards the risks to which they may be exposed, so that they have the confidence and skills to face and deal with them should they arise. The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how we do this.

School e-Safety Policy

The school has an appointed e-Safety coordinator / officer who is also Safeguarding lead (Jane Farren).

Our e-Safety Policy has been written by the school, building on the Gloucestershire Children and Young Peoples' Directorate and Government guidance. It has been agreed by the senior management team and approved by governors.

The e-Safety Policy will be reviewed annually.

Why is Internet Use Important?

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 information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access

Many pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet use benefit Education?

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;
- educational and cultural exchanges between pupils world-wide;
- 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 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 the Local Authority and DCSF; access to learning wherever and whenever convenient.

How can Internet Use Enhance Learning?

- The school Internet access will be designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity.

- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Authorised Internet Access

- The school will maintain a current record of all staff and pupils who are granted Internet access.
- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- Parents will be informed that pupils will be provided with supervised Internet access.
- Parents will be asked to sign and return a consent form for pupil access.

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the Local Authority helpdesk via the e-safety coordinator or network manager.
- School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Email

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Whole class or group e-mail addresses should be used in school.
- Access in school to external personal e-mail accounts may be blocked.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

Social Networking

- Schools should block/filter access to social networking sites and newsgroups unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils should be advised not to place personal photos on any social network space.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.

Filtering

The school will work in partnership with the Local Authority and the Internet Service Provider to ensure filtering systems are as effective as possible.

Video Conferencing

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupils' age.

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used for personal use during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Staff will be issued with a school phone where contact with pupils is required.

Published Content and the School Web Site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
- The head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupils' Images and Work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified by name.
- Pupils' full names will not be used anywhere on the Web site, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- Work can only be published with the permission of the pupil and parents.

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Local Authority.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. Children's biometric information will only be processed in accordance with the Protection of Freedoms Act 2012.

Assessing Risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Gloucestershire County Council can accept liability for the material accessed, or any consequences of Internet access.
- The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

Handling e-safety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.

- Any complaint about staff misuse must be referred to the Head Teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Communication of Policy

Pupils

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that Internet use will be monitored.

Staff

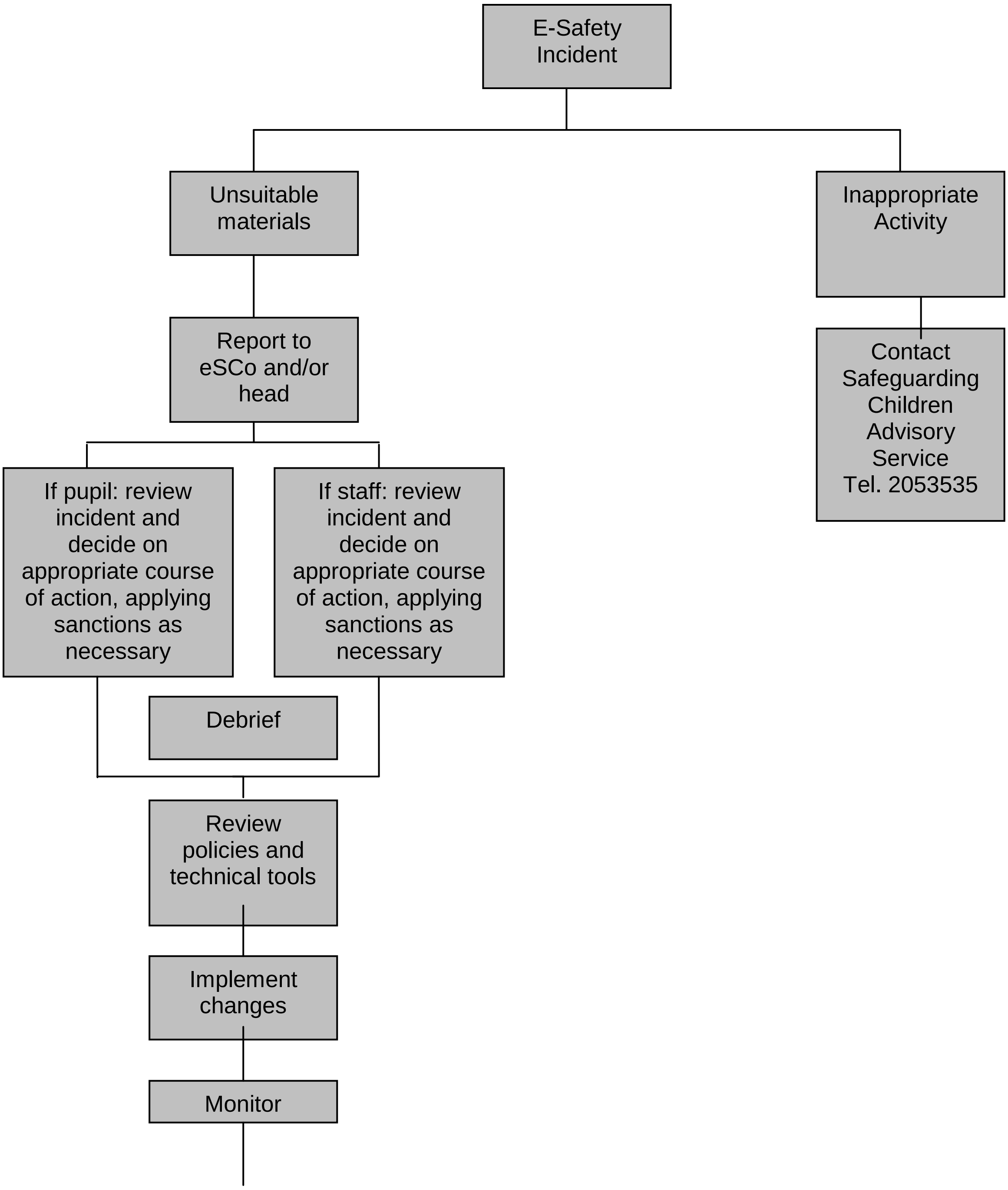
- All staff will be given the School e-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Parents

- Parents' attention will be drawn to the School e-Safety Policy in newsletters and on the school Web site.

Appendix A

Flowchart for responding to e-safety incidents in school


E-Safety Incident
Unsuitable materials
Inappropriate Activity
Report to eSCo and/or head
Contact Safeguarding Children Advisory Service Tel. 2053535
If pupil: review incident and decide on appropriate course of action, applying sanctions as necessary
If staff: review incident and decide on appropriate course of action, applying sanctions as necessary
Debrief
Review policies and technical tools
Implement changes
Monitor

Adapted from Becta – E-safety 2005

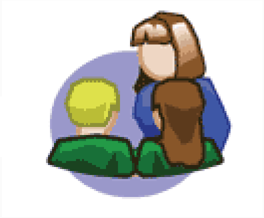
Appendix B

e-Safety Rules

Think then Click

We ask permission before using the internet.

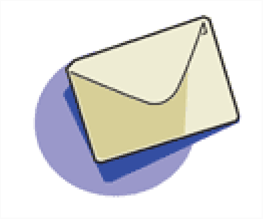
We only use websites our teacher has chosen.



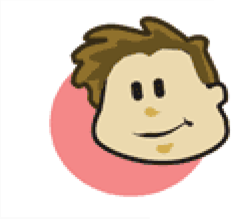
We tell an adult if we see anything we are uncomfortable with.

We immediately close any webpage we are uncomfortable with.

Strive Think Act Respect Shine



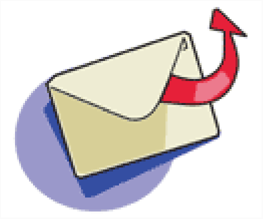
We only email people an adult has approved.



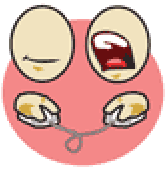
We send e-mails that are polite and friendly.

We never give out personal information or passwords.

We never arrange to meet anyone we don't know.



We do not open e-mails sent by anyone we don't know.



We do not use Internet chat rooms.

Edit this poster for display near computers.

Our School

e-Safety Rules

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

Parent's Consent for Web Publication of Work and Photographs

I agree that my son/daughter's work may be electronically published. I also agree that appropriate images and video that include my son/daughter may be published subject to the school rule that photographs will not be accompanied by pupil names.

Parent's Consent for Internet Access

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

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

Signed:	**Date:**
Please print name:	

Strive Think Act Respect Shine

Please complete, sign and return to the school

Appendix C

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	*							*
Use of mobile phones in lessons				*				*
Use of mobile phones in social time	*							*
Taking photos on mobile phones or other camera devices				*				*
Use of hand held devices eg PDAs, PSPs	*							*
Use of personal email addresses in school, or on school network	*							*
Use of school email for personal emails		*						*
Use of chat rooms / facilities				*				*
Use of instant messaging				*				*
Use of social networking sites				*				*
Use of blogs				*				*

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 need to be aware that email communications may be monitored**
- **Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.**
- ***Any digital communication between staff and students / pupils or parents / carers must be professional in tone and content.***

- Students / pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Appendix D

Unsuitable / inappropriate activities

The school believes that activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in or out of school when using school equipment or systems. The school policy restricts certain internet usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**child sexual abuse images**					▪
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					▪
	adult material that breaches criminal legislation in the UK					▪
	criminally racist material in UK					▪
	pornography				▪	
	promotion of any kind of discrimination				▪	
	promotion of racial or religious hatred				▪	
	threatening behaviour, including promotion of physical violence or mental harm				▪	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				▪	
Using school systems to run a private business					▪	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the school					▪	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					▪	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					▪	
Creating or propagating computer viruses or other harmful files					▪	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet					▪	
On-line gaming (educational)			*			

On-line gaming (non educational)				*	
On-line gambling				*	
On-line shopping / commerce				*	
File sharing			*		
Use of social networking sites				*	
Use of video broadcasting eg Youtube				*	

Appendix E

Students / Pupils Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		▪	▪	▪		*	*	*	*
Unauthorised use of non-educational sites during lessons	*							*	
Unauthorised use of mobile phone / digital camera / other handheld device	*	*				*		*	
Unauthorised use of social networking / instant messaging / personal email	*	*			*	*	*	*	
Unauthorised downloading or uploading of files	*	*			*	*	*	*	
Allowing others to access school network by sharing username and passwords	*	*			*	*	*	*	
Attempting to access or accessing the school network, using another student's / pupil's account	*	*			*	*	*	*	
Attempting to access or accessing the school network, using the account of a member of staff		*			*	*		*	
Corrupting or destroying the data of other users		*			*	*	*	*	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature			*		*	*	*	*	*
Continued infringements of the above, following previous warnings or sanctions			*		*	*	*		*
Actions which could bring the school into disrepute or breach the integrity of the ethos			*		*	*	*	*	*

of the school									
Using proxy sites or other means to subvert the school’s filtering system	*	*	*			*	*	*	*
Accidentally accessing offensive or pornographic material and failing to report the incident	*	*	*		*	*		*	
Deliberately accessing or trying to access offensive or pornographic material			*	*	*	*	*	*	*
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			*	*	*	*	*	*	*

Staff

Actions / Sanctions

Incidents:	Refer to line managerr	Refer to Headteacher	RRefer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		▪	▪	▪		▪		
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email		▪	▪			▪		
Unauthorised downloading or uploading of files		▪		▪		▪		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person’s account		▪	▪		▪			
Careless use of personal data eg holding or transferring data in an insecure manner		▪	▪		▪	▪		
Deliberate actions to breach data protection or network security rules		▪	▪	▪	▪		▪	▪
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		▪	▪	▪		▪	▪	▪
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		▪	▪		▪		▪	▪
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		▪	▪	▪	▪		▪	▪
Actions which could compromise the staff member’s professional standing		▪	▪			▪		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		▪	▪			▪		
Using proxy sites or other means to subvert the school’s filtering system		▪				▪		

Accidentally accessing offensive or pornographic material and failing to report the incident		▪	▪			▪		
Deliberately accessing or trying to access offensive or pornographic material		▪	▪	▪			▪	▪
Breaching copyright or licensing regulations		▪	▪			▪		
Continued infringements of the above, following previous warnings or sanctions		▪	▪				▪	▪

Appendix G

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Headteacher of Norton Primary School or the E-Safety coordinator.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- Mobile phones are not to be visible in any teaching areas and are not to be used during teaching hours.
- All staff of the school will not have any pupils of the school as friends on Social Networks. Teaching staff will not have any parents of the school as friends on Social Networks.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
- I will not install any hardware or software without permission from the Head.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent from the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the Headteacher.
- I will respect copyright and intellectual property rights.
- I will support and promote the school's E-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

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

Signed: ……………………………… Capitals: ……………………… Date: ………

Accepted for school: …………………………… Capitals: …………………………

E-Safety Audit –

This quick self-audit will help the senior management team (SMT) assess whether the e-safety basics are in place.

Has the school an e-Safety Policy that complies with CYPD guidance?	yes
Date of latest update: September 2012	
The Policy was agreed by governors on: September 2012	
The Policy is available for staff: policy folder, server, Keeping Norton Children Safe folder(staff room)	
And for parents at: Policy folder, Website	
The designated Child Protection Teacher/Officer is: Jane Johnson	
The e-Safety Coordinator is: Miss Cundick	
Has e-safety training been provided for both pupils, parents and staff?	Yes
Is the Think U Know training being considered?	Yes
Do all staff sign an ICT Code of Conduct on appointment?	Yes
Do parents sign and return an agreement that their child will comply with the School e-Safety Rules?	Yes
Have school e-Safety Rules been set for pupils?	YES
Are these Rules displayed in all rooms with computers?	Yes
Internet access is provided by an approved educational Internet service provider and complies with DCSF requirements for safe and secure access.	Yes
Has the school filtering policy been approved by the SMT?	Yes
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Yes

The school will monitor the impact of the policy using:

- Logs of reported incidents
- SWGfL monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys / questionnaires of
  - pupils - CEOP ThinkUknow survey
  - parents / carers
  - staff