Toft Hill Primary School
E-Safety Policy

Signed _____Head Teacher

Signed_____ Chair of Governors

Date of review: Feb 2016

J. Stobbs 2013

Toft Hill Primary School: e-Safety and Acceptable Use Policy

Policy writing and review

Our e-Safety and Acceptable Use Policy has been written by the school taking account of Durham Schools e-safety Policy, advice from Kent County Council and Government advice. Internet use includes the Durham Learning Gateway by staff and pupils at school and home. Our school policy has been agreed by the Senior Leadership Team and approved by the Governors. Our school has formed an e-safety committee which includes the e-safety coordinator, the head teacher, deputy head teacher and an appointed member of the Governing body.

E-safety coordinator – Mr Mark Dickinson
E-safety Governor – Mrs Michelle Telford

Policy approved by Head Teacher:…….Date:……..

Policy approved by the Governing Body:……. (Chair of Governors)

Date:…….

The policy will be reviewed annually.

Teaching and Learning

1. 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 functions;
- The internet is an essential part of 21st Century life for education, business and social interaction;
- The internet is part of the statutory curriculum and is a necessary tool for learning;
- Internet access is an entitlement for pupils who show a responsible and mature approach to its use.

2. How does Internet use benefit education?

Benefits of using the Internet in education include:

- Access to worldwide educational resources including museums and art galleries;
- 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, education 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 systems updates;
- Exchange of curriculum and administrative data with LA and DfE;
- Access to learning wherever and whenever convenient.

3. How can Internet use enhance learning?

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of the pupils;
- Pupils will be taught what Internet use is acceptable and what is not. They will be given clear objectives for Internet use and the importance of e-safety. This will be done through assemblies and through direct teaching in ICT lessons;
- Internet access, including the use of the learning gateway, will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and the age of the pupils;
- Staff should guide pupils in on-line activities that will support the 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.

4. How will pupils learn to evaluate Internet content?

- The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law;
- 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 encouraged to minimise the screen to hide any material that they know is unsuitable for viewing until it can be dealt with by the class teacher. Unsuitable sites must be reported to the Internet Service Provider via the ICT coordinator;
- Pupils will be taught to use search engines appropriately for their age.
- Training should be available to staff in the evaluation of Web materials and methods of developing pupils' critical attitudes.

Managing Information Systems

1. How will information systems security be maintained?

The Internet is both an invaluable resource for education, business and social interaction but it is also holds many potential risks.

- The security of the school information systems and users will be regularly reviewed;
- Virus protection will be updated regularly;
- The school will comply with the terms of the data protection act (see separate Data Protection Policy)

2. How will e mail be managed?

The current email system gives anonymity to pupils through the email address they are given. The pupil's first name and the initial letter of their surname are used with a number e.g. b.s1000@durhamlearning.net

This means the pupil's full name is not available, nor is the location of their school. This system combines the best of practice in pupil email account names. The service is also filtered.

- Pupils may only use approves e mail accounts for school purposes.
- Pupils must immediately tell a designated member of staff if they receive 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.
- Access in school to external personal e-mail accounts may be blocked
- Excessive social e-mail use can interfere with learning and may be restricted
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper
- The forwarding of chain messages is not permitted.

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 will not be published
- The head teacher, or their nominee, will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.

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. This is done through he school's photographic policy, parents give permission for the whole of the child's school career.

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

- Newsgroups will not be made available to pupils unless an educational requirement for their use has been demonstrated
- The school will educate its pupils on the safe use of social networking as part of its curriculum
- Pupils will be advised never to give out personal details of any kind that might identify them
- Pupils and parents will be advised that the use of social networking sits outside of school brings a range of dangers for primary aged pupils
- Staff personal use of social networking, social media and personal publishing sites will be outlined in the school Acceptable Use Policy.

6. How will filtering be managed?

- The school's broadband access will include filtering
- The school's e-safety committee will consider requests making changes to the filtering
- The school with DCC to review filtering
- There is a clear system in place for reporting breaches of filtering. All members of the school community (staff and pupils) are aware of this procedure as it forms part of the e-safety curriculum
- 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

- Regular checks will be made to ensure that filtering methods selected are effective.

7. How will videoconferencing be managed?

- 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.

8. ***How are emerging technologies managed?***

- Emerging technologies will be examined for educational benefit and a risk assessment carried out before use in school is allowed
- Use of personal devices, by staff and pupils, is outlined in Acceptable Use Policy

9. How should personal data be protected?

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

Policy Decisions

1. How will internet access be authorised?

- All staff will read and sign the Acceptable Use Policy before using any of the 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 who require access to the schools network or internet access will be asked to sign and read an Acceptable Use Policy
- Parents will be informed that pupils will be provided with supervised internet access appropriate to their age and ability
- When considering access for vulnerable pupils (such as children with special educational needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

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 DCC can accept liability for the material accessed, or any consequences resulting from Internet use
- The use of computer systems without permission or for inappropriate purposes could be constituted a criminal offence under the Computer Misuse Act 1990
- Methods to identify, assess and minimise risks will be reviewed regularly
- The head teacher will ensure that the Internet Policy is implemented and compliance with the policy monitored.

3. How will the school respond to 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, cyber bullying etc)
- The e-safety Coordinator will record all reported incidents and actions taken in the school's e-safety incident log and in any other relevant areas e.g. Bullying or Child protection

- The designated Child protection Coordinator will be informed of any e-safety incidents involving Child Protection concerns, which will then be escalated appropriately
- The school will manage e-safety incidents in accordance with the school behaviour policy where appropriate

5. How will e-Safety complaints be handled?

- Complaints about Internet misuse will be dealt with under the School's complaint procedure
- Any complaint about staff misuse will be referred to the head teacher
- All complaints and incidents will be recorded by the school, including any actions taken
- Parents and pupils will need to work in partnership with the school to resolve 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 any other members of the community.

6. How is the Internet used across the community?

- 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 an AUP for any guest who needs to access the school computer system or internet on site.

7. How will cyber bullying be handled?

- Cyberbullying (along with other forms of bullying) of any member of the school community will not be tolerated. (See school's Anti-bullying policy)
- All incidents of cyberbullying reported to the school will be recorded
- 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
- The school will support anyone within the community affected by cyberbullying
- Sanctions for those involved in cyberbullying may be used in accordance to the school's Anti-bullying, Behaviour and Acceptable Use Policies. Parents will be informed.

8. How will mobile phones and personal devices be handled?

- The use of mobile phones and other personal devices by pupils and staff in school will be decided by school and covered in the school Acceptable Use Policy
- Electronic devices of all kinds that are brought into school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items.

Communication Policy

1. How will the policy be introduced to pupils?

- Rules for Internet access and pupils' Acceptable Use Policy will be posted in all rooms where computers are used

- Pupils will be informed that Internet use will be monitored
- Instruction in responsible and safe use should precede Internet access
- Lessons on e-safety will form part of the regular teaching of Computing, and this will also be addressed on a whole school level through assemblies
- Pupils are expected to sign Acceptable Use agreements.

2. How will the policy be discussed with staff?

- The e-safety Policy will be formally provided for and discussed with all members of staff
- To protect all staff and pupils, the school will implement Acceptable Use Polices
- 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 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.

3. How will parents support be enlisted?

- Parents' attention will be drawn to the school e-safety Policy in newsletters, the school brochure and the school web-site
- A partnership approach to e-safety in the home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations, practical sessions and suggestions for safe home Internet use, or highlighting e-safety at other attended events e.g. parents' evening.
- 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 Acceptable Use Policy for pupils and discuss its implications with their children.
- Advice on useful resources and websites will be made available to parents via curriculum letters and the school website.
- Interested parents will be referred to organisations such as NCH Action for Children.

Pupils e-safety agreement

Keeping me safe at home and at school

We check with a grown up before using the internet
e.g. on a computer, tablet or phone

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 on the internet.

We will not bring mobile phones to school

J. Stobbs 2013

Pupils e-safety contract

Please complete, sign and return to the school secretary

Pupil:	***Class:***

Pupil's Agreement

I have listened to and understood the pupil's e-safety agreement, and will follow the rules which are there to keep me 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:

Pupils' e-safety agreement

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

J. Stobbs 2013

- 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 use Mobile Phones during the school day or at any after school event.
- 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 stick to 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:	

Toft Hill Primary School

Acceptable Use Policy

As a professional organisation with responsibility for children's safeguarding it is important that all staff 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 and offline communication technologies and access devices. Examples include mobile phones, PDAs, digital cameras, email and social media sites**.**

- Staff Mobile Phones are allowed in school, but are not allowed to be used in sensitive areas (EYFS, Cloak Rooms, Toilets, When children are changing, Swimming). Mobile phones should only be used for communication when not working with children.

- Cameras on personal phones will not be used to take pictures of children in any circumstances.

- In the unlikely event of needing to contact a parent directly a school mobile phone will be issued to the member of staff concerned.

- 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. 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 (A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one 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 (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the school. Secure means of transporting data are either an encrypted memory stick or use of the DLG. 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. Where possible I will use the School Learning Platform 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 Coordinators, J Stobbs and L Paley and/or the e-Safety Coordinator, M Dickinson as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to M Dickinson, the e-Safety Coordinator and 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 (ITSS) 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. *This would include any relatives of current pupils that are my "friends" on a social media site.*

- 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 practise online either in school or off site, then I will raise them with the e-Safety Coordinator, M Dickinson, or 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 information 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……..

Copy of letter to be sent home to parents and carers

Dear Parents

Responsible Use of the Internet

As part of your child's curriculum and the development of Computing skills, our school provides supervised access to the Internet. We believe that the effective use of the Internet and e-mail is worthwhile and an essential skill for children as they grow up in the 21st Century.

E-safety is a high priority in school. In order for pupils to use the Internet at home and in school we need them to be aware of the Internet rules and how to remain safe.

Although there are concerns about pupils having access to undesirable materials, we have taken positive steps to reduce this risk in school. E-safety is a high priority in school and we would like to ensure children are also protected in their use of the Internet at home. Our school Internet provider operates a filtering system that restricts access to inappropriate materials. This may not be the case at home and we can provide references to information on safe Internet access if you wish.

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the school cannot be held responsible for the nature or content of materials accessed through the Internet. The school will not be liable for any damages arising from your child's use of the Internet facilities.

We work with children to develop their understanding of how useful the Internet can be and also how dangerous. Please would you read the attached **'Acceptable Use Policy'** and discuss this with your child, then return the signed agreements.

If you have any questions or concerns, do not hesitate to contact me.

Yours sincerely

Mrs J Stobbs

Toft Hill Primary School E-safety Audit

This self-audit will be completed by the E-safety committee

	Y/N
Has the school an e-safety policy that complies with Durham County Guidance?	
Date of last update:	
Internet policy last updated on:	
Are policies available for parents/carers?	
Member of SLT responsible:	
Member of governing body responsible:	
Designated child-protection coordinator:	
Has e-safety training been provided for staff and pupils?	
Is there a clear procedure for response to an incident of concern?	
Have e-safety materials been obtained and used?	
Do all staff sign a Code of Conduct for ICT	
Are pupils aware of e-safety rules?	
Are e-safety rules displayed in all rooms where there is access to the computer, and expressed in a form that is accessible to all pupils?	
Do parents/carers sign and return agreements about safe Internet use?	
Are all staff, pupils, parents and visitors aware that their child will comply with the school e-safety rules?	
Is personal data collected, stored and used according to the principles of the Data Protection Act?	
Is Internet access provided by an approved educational Internet service provider which complies with DCSF requirements?	
Has the school-level filtering been designed to reflect the educational objectives and approved by SLT?	

Audit date:_____

Signed:_____

_____

J. Stobbs 2013