St Thomas's CE Primary School

E-Safety Policy

School:	St Thomas CE Primary School
Date adopted by Governing Body:	February 2014 Reviewed Feb 2017
Signed: (Chair of Governors)	
Signed: (Headteacher)	

1. Introduction

At St Thomas's Primary School we understand the responsibility we have to educate our pupils on e-safety issues; teaching them appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

St Thomas's Primary School has a whole school approach to the safe use of ICT and creating this safe learning environment includes three main elements:

- an effective range of technological tools
- policies and procedures, with clear roles and responsibilities
- a comprehensive e-safety programme for pupils, staff and parents.

Our e–Safety Policy has been written by the school, building on government guidance. It has been agreed by the Senior Leadership Team, teaching staff and teaching assistants and approved by governors.

2. Roles and Responsibilities

E-Safety is recognised as an essential aspect of St Thomas's Primary School.

Judith Jones (Headteacher) has overall responsibility, in her absence Kath Crawley (Deputy Head). Also Emma Ellis (Computing Leader) and Judith Kerr (School Business Manager) are the named staff for staff, parents and children to report any concerns.

It is the role of these staff members to keep abreast of current issues and guidance by attending regional computing leadership meetings and up-dates from WSCB and DfE.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and follow school e-safety procedures.

All staff should be familiar with the school's policy including:

- safe use of e-mail
- safe use of the Internet
- safe use of the school network, equipment and data
- safe use of digital images and digital technologies, such as mobile phones and digital cameras
- publication of pupil information/photographs on the school website
- their role in providing e-safety education for pupils.

(list of related policies at end of document)

Staff are reminded/updated about e-safety regularly and new staff receive information on the school's acceptable use policy as part of their induction.

Managing the school e-safety messages

- We endeavour to embed e-safety messages across the curriculum whenever the internet and/or related technologies are used.
- The e-safety policy will be shared with new staff as part of their induction.
- E-safety posters will be prominently displayed.

3. Curriculum

Computing and online resources are increasingly used across the curriculum. We believe it is essential for e-safety guidance to be given to the pupils on a regular and meaningful basis.

We continually look for new ways to promote e-safety.

- We provide opportunities within a range of curriculum areas to teach about e-safety.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally, when opportunities arise and as part of the curriculum.

- Pupils are taught about copyright and respecting other people's information, images etc. through discussion, modelling, and activities as part of the Computing curriculum.
- Pupils are aware of the impact of online bullying through worships and computing lessons and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the Computing curriculum

4. Managing Internet Access

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education as well as a potential risk to young people.

Students will have supervised access to Internet resources through the school's fixed and mobile technology.

Staff will preview any recommended sites before use.

Raw image searches are discouraged when working with pupils.

If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise any further research.

Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.

If staff or pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to the

Headteacher or computing leader.

It is the responsibility of the school, by delegation to the network manager, to ensure that anti-virus protection is installed and kept up-to-date on all school machines.

Any changes to filtering must be authorised by a member of the senior leadership team.

5. Security and Data Protection

The school and all staff members comply with the Data Protection Act 1998. Personal data will be recorded, processed, transferred and made available according to the act. Password security is essential for staff, particularly as they are able to access and use pupil data. Staff have secure passwords which are not shared with anyone.

6. E-Safety Complaints/Incidents

As a school we take all precautions to ensure e-safety at all times.

- Complaints of Internet misuse will be dealt with under the School's Complaints Procedure.
- Any complaint about staff misuse must be referred to the head teacher.
- All e–Safety complaints and incidents will be recorded by the school — including any actions taken.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary and child protection procedures.

7. Cyber bullying

Cyber bullying (along with all forms of bullying) will not be tolerated in school. Full details are set out in the school's policy on anti-bullying.

- There will be clear procedures in place to support anyone affected by Cyber bullying.

- There will be clear procedures in place to investigate incidents or allegations of Cyber bullying:
- 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 appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Sanctions for those involved in Cyber bullying may include:
    - The bully will be asked to remove any material deemed to be inappropriate or offensive.
    - A service provider may be contacted to remove content.
    - Internet access may be suspended at school for the user for a period of time.
    - Parent/carers may be informed.
    - The Police will be contacted if a criminal offence is suspected.

8. Management of E-mail

- Pupils may only access approved email accounts.
- Pupils must immediately tell a teacher 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.
- Whole class or group email addresses will be used in school for communication to outside organisations.
- 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.

- Staff should not use personal email accounts during school hours on school hardware or send sensitive information at anytime.

9. Publishing of pupils images or work

- 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 of pupils are electronically published.
- Pupils work can only be published with their permission or the parents.

10. Management of social networking and social media

- Pupils will discuss how to be safe on social network sites.
- They 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 and email addresses, full names of friends/family, specific interests and clubs etc.
- Pupils should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location.
- 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 by making profiles private.
- Pupils are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

10. Staff use of I pads, social media and mobile phones

- Mobile phones will not be used during lessons or formal school time (eg. break duty). The sending of abusive or inappropriate text, picture or video messages is forbidden.
- No photographs should be taken on personal telephones or cameras.
- Classroom I pads will not be taken off school premises except when on an educational visit or used for personal activity.
- All apps and software must be agreed by the network manager or computing leader before downloading.
- Class pages on the school website are set up to inform parents about school activities, class projects and upcoming events.
- Communication with parents via Twitter will not be permitted.
- St Thomas's School Twitter account should not be used for personal use.

Policy to be read alongside the E-safety Policy:

- Staff code of conduct
- IT security guidance
- Policy for Data and IT security
- Guidance for Schools on Acceptable Usage of IT
- Social Media Policy for Employees in Schools
- Safeguarding Policy
- Anti-bullying Policy