

THUNDERSLEY PRIMARY SCHOOL

e-safety Policy



Member of staff Responsible	<i>Steve Mackay</i>
Policy produced	<i>July 2017</i>
Policy agreed/last reviewed	<i>December 2017</i>
To be reviewed	<i>Autumn 2019</i>
Other Policies Related	<i>Child Protection Policy; ICT policy; staff acceptable use policy</i>
Other Paperwork Attached (appendix)	<i>SMART Poster for display in classrooms</i>

INTRODUCTION

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in Thundersley Primary School are bound. This e-safety policy will help ensure safe and appropriate use both in and out of school. The development and implementation of this strategy involves all the stakeholders in a child's education from the headteacher and governors to the senior management team, subject manager and classroom teachers, support staff, parents/carers, members of the community and the pupils themselves

Online 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 online safety policy will operate in conjunction with other policies including those for Behaviour, Bullying, Curriculum, Data Protection and Safeguarding.

Good Habits

Online 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 policies.
- Sound implementation of online safety in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband including the effective management of content filtering.

The use of these exciting and innovative tools in Thundersley Primary School and at home has been shown to raise educational standards and promote pupil achievement.

However, the use of these new technologies can put young people at risk within and outside the school. 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.
- The risk of being subject to terrorist and extremist material.

Many of these risks reflect situations in the off-line world and this e-safety policy is used in conjunction with other school policies (eg behaviour, anti-bullying and child protection policies).

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 to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

Thundersley Primary School demonstrates the necessary safeguards to help ensure that we have done everything that could reasonably be expected of us to manage and reduce these risks.

Roles and Responsibilities

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. The role of the

E-Safety Governor will include:

- *Regular meetings with the E-Safety Lead*
- *Regular monitoring of e-safety incident logs*
- *Regular monitoring of filtering/change control logs*
- *Reporting to relevant Governors meeting*

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of The Thundersley Primary School community, though the day to day responsibility for e-safety will be delegated to the E-Safety Lead.
- The Headteacher/Senior Leadership Team are responsible for ensuring that the E-Safety Lead and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- The Headteacher/Senior Leadership Team will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role.
- The Senior Leadership Team will receive regular monitoring reports from the e-safety Lead.
- The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

E-Safety Lead:

- Takes day to day responsibility for e-safety issues and establishes and reviews the school's e-safety policies/documents
- They will ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- They will provide training and advice for staff. This will include radicalisation.
- Liaise with school ICT technical staff

- To receive reports of e-safety incidents and create a log of incidents to inform future e-safety developments,
- Meet regularly with the E-Safety Governor to discuss current issues, review incident logs and filtering/change control logs
- Attend relevant meeting/committee of Governors
- Report regularly to the Senior Leadership Team
- They ensure the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- Ensures the school meets the e-safety technical requirements outlined in any relevant
- e-Safety Policy and guidance
- Ensures users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- Keep the Senior Leadership Team are informed of issues relating to the filtering applied by the network
- Keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- Monitors the use of the network/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the ICT leader for investigation
- Monitors software/systems are implemented and updated as agreed in school policies

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- They read, understand and sign the school Staff Acceptable Use Policy
- They report any suspected misuse or problem to the ICT Co-ordinator for investigation
- Digital communications with pupils should be on a professional level *and only carried out using official school systems*
- E-safety issues are embedded in all aspects of the curriculum and other school activities
- They report any suspected use of terrorist or extremist ideas originating from computer access. This information will then be referred to the head teacher.
- Students/pupils understand and follow the school e-safety and acceptable use policy
- They monitor ICT activity in lessons, extra-curricular and extended school activities
- They are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- In lessons, where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Person

Should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying

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 intend to do this, while also addressing wider educational issues in order to help young people (and their parents/carers) to be responsible users and stay safe while using the internet

Pupils

- Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems.
- Have a good understanding of research skills.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking/use of images and on cyber-bullying.
- Need to understand the risks associated with terrorism and develop the knowledge and skills to be able to challenge extremist views.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's e-Safety Policy covers their actions out of school, if related to their membership of the school.

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet mobile devices in an appropriate way. Thundersley Primary School will take every opportunity to help parents understand these issues through *parents' evenings, newsletters, letters, website and information about safety campaigns*. Parents and carers will be responsible for:

- Endorsing (by signature)
- Accessing the school website/on-line pupil records in accordance with the relevant school Acceptable Use Policy.

Policy Statements

Education-Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision.

Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience. E-Safety education will be provided in the following ways:

- A planned e-safety programme will be provided as part of ICT/PHSE/other lessons and should be regularly revisited - this will cover both the use of ICT and new technologies in school and outside school
- Key e-safety messages will be reinforced as part of a planned programme of assemblies and activities
- Pupils will be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information
- Pupils will be helped to understand the need for the Pupil User Agreement and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Through the promotion of British Values, the pupils will be taught to challenge extremist views when using material accessed on the internet
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Staff will act as good role models in their use of ICT, the internet and mobile devices
- Education - Parents/Carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online experiences.

Thundersley Primary School will therefore seek to provide information and awareness to parents and carers through:

- *Letters, newsletters, web site,*
- *Parents meetings*
- *Reference to websites (e.g. UK Safer Internet Centre)*

Education and Training - Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff.
- An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the performance management process.

- All new staff will receive e-safety training, ensuring that they fully understand the school's e-safety policy and Acceptable Use Policies.
- The E-Safety Lead will receive regular updates through attendance at training sessions and by reviewing guidance documents.
- This e-safety Policy and its updates will be presented to and discussed by staff in staff meetings and INSET days.
- The E-Safety Lead will provide advice, guidance and training as required to individuals as required.
- Training - Governors
- Governors should take part in e-safety training sessions;
- Participation in school training/information sessions for staff and parents
- Technical - infrastructure/equipment, filtering and monitoring
- The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:
- School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the E-Safety Policy and Acceptable Use Policy and any relevant guidance.
- There will be regular reviews and audits of the safety and security of school ICT systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, annually.
- All users will be provided with a username and password.
- The "administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher and kept in a secure place.
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service.
- In the event of the Network Manager needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher.
- Any filtering issues should be reported immediately to the Local Authority.
- Requests from staff for sites to be removed from the filtered list will be considered by the Headteacher. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly.
- Remote management tools are used by staff to control workstations and view users activity
- An appropriate system is in place (CEOP Reporting Button) for users to report any actual/potential e-safety incident to the ICT Co-ordinator.

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed Acceptable Use Policy is signed by all staff.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Curriculum

- E-safety will be a focus in all areas of the curriculum and staff will reinforce e-safety messages in the use of ICT across the curriculum.
- In lessons where internet use is pre-planned, it is best practice that pupils will be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, eg using search engines, staff will be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs and discrimination) that would normally result in internet searches being blocked.
- Pupils will be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Are aware of the risks posed by the online activity of extremist and terrorist groups.

- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.
- When personal data is stored on any portable computer system, USB stick or any other removable media:
 - The data must be encrypted and password protected.
 - The device must offer approved virus and malware checking software.
 - The data must be securely deleted from the device once its use is complete.

S

SAFE

Keep safe by being careful not to give out personal information – such as your full name, email address, phone number, home address, photos or school name – to people you are chatting with online.



M

MEETING

Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.



A

ACCEPTING

Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!



R

RELIABLE

Information you find on the internet may not be true, or someone online may be lying about who they are.



T

TELL

Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

THINK
U
KNOW
CO.UK

You can report online abuse to the police at www.thinkuknow.co.uk

