St Thomas á Becket CE (Aided) Primary School

E-safety, social media and use of camera policy

Policy agreed	April 2016
Policy published	April 2016
Next review date	April 2018
Approved by	FGB
May be delegated to committee, individual governor or Head teacher	
Policy linked with:	

Background / rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

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 schools are bound. The development of this strategy has involved the head teacher, governors, classroom teachers, support staff, parents, members of the community and the pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student 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.

Many of these risks reflect situations in the off-line world and it is essential that 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 students' / 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.

The 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 and other communications technologies for educational, personal and recreational use.

Scope of the policy
This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities
The following section outlines the roles and responsibilities for this policy of individuals and groups within the school:

A) E-Safety

Governors
Governors are responsible for the approval of this policy (including e-safety) and for reviewing the effectiveness of the policy. This will be carried out by the Education Committee.

Head teacher:

- The Head teacher is responsible for ensuring the safety (including e-safety) of members of the school community.
- The Head teacher and a Governor 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.
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents.
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff.
- liaises with the Local Authority.
- liaises with school ICT technical support company
- monitors any reports of e-safety incidents.
- ensures that a robust filtering systems is in place and that that the school's ICT infrastructure is secure and is not open to misuse.
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed.
- SWGfL is informed of issues relating to the filtering applied by the Grid Keeps 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.

Teaching & 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 have read and understood this policy and signed to that effect (signed copies to be kept on file).
- they report any suspected misuse or problem to the head teacher.
- 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.
- pupils understand and follow the school e-safety and acceptable use policy
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- 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 students / 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 person for child protection
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

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. (At KS1 it would be expected that parents / carers would sign on behalf of the pupils)
- Through teaching in KS2 they should:
- develop a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- 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.
- 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. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature. Parents and carers will be responsible for:

- endorsing (by signature) the Pupil Acceptable Use Policy.
- ensuring that they do not comment on specific children or incidents or about school staff (in connection with any aspect of their work) on any social media website).
- accessing the school website in accordance with the schools usage guidelines: that this page is for providing information about school activities

and questions relating to this and not for discussion of children, incidents or staff with the understanding that any such posts will be deleted by the administrator.

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 should 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.
- In KS2: Pupils should be taught in lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be helped to understand and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Rules for use of ICT systems / internet will be posted in all rooms and displayed on log-on screens.
- Staff should act as good role models in their use of ICT, the internet and mobile devices.

Education & 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:

- 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.
- All new staff should receive e-safety information as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies
- The Head teacher will receive regular updates through attendance at LA / other information / training sessions and by reviewing guidance documents released by BECTA / SWGfL / LA and others.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Head teacher will provide advice / guidance / training as required to individuals as required.

Training – Governors

Governors should be take part in e-safety training / awareness sessions, as part of a governing body meeting or as part of in school training / information sessions for staff or parents.

Technical – infrastructure / equipment, filtering and monitoring

- Servers, wireless systems and cabling must be securely located and physical access restricted

- Only the head teacher as access to her personal files, all teaching staff and the admin officer have access to staff share and pupils and teachers have access to student share.
- All users (at KS2 and above) will be provided with a username and password
- The “master / administrator” passwords for the school ICT system, used by the external Network Manager must also be available to the Head teacher and kept in a secure place (eg school safe).
- Users will be made responsible for the security of their username and password and 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 provided by SWGfL.
- In the event of the need to switch off the filtering on a computer to access teaching materials this must be reset by the teacher who disabled it at the end of the session.
- Any filtering issues should be reported immediately to the broadband provider.
- Appropriate security measures are in place supplied by external ICT managers 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.
- Children are allowed to bring memory sticks to school to transport homework or material pre-agreed by a member of staff. These memory sticks should be kept by a teacher and only used as agreed by that teacher
- Teaching staff who need to use their class laptop for school work may take them home to use provided they are only used for school work.

B) Camera and photographic use

The use of cameras is considered an essential and integral part of everyday school life.

Cameras are frequently used for recording children taking part in class and school activities and are often used by adults and teachers as a teaching aid.

The purpose of this policy is to ensure that there are clear guidelines regarding the taking of photographs and that there is no inappropriate or potential for inappropriate use of photographs taken at school from the use of mobile phones, photographs or personal cameras.

Parents' consent is sought for the use of photographs when a child joins the school and this will last for the duration of their stay. Parents retain the right to withdraw their consent at any time but need to do so in writing to the head teacher. These photographs will be used for recording activities and may also be used on the school website or sent for publication in newspapers.

Use of cameras/video cameras in school:

Photographs or videos used for recording or teaching will only be stored on the school computers.

On no account should photographs be taken on mobile phones within the school.

No photographs taken in school or at school events will be put on social networking sites.

No personal cameras including phone cameras are to be used by staff on site– (no children are allowed to bring personal cameras into school).

Mobile phones with cameras should not be switched on while children are in the classroom including music and games sessions (unless express permission has been sought from the Headteacher).

Staff may carry mobile phones on school trips but should not use these for taking photographs

Supply staff, students and class helpers will be made aware of the content of this policy.

Students' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Parent's use of cameras/videos

Parents will be invited to record their child' inclusion in events such as sports' day/productions on the understanding that they will not publish any material on the internet. We do not allow flash photography in any indoor school events except for arranged opportunities at the end.

C) Social Media

Whilst recognising the benefits of the range of social media sites and the benefits of these forms of communication it is crucial that staff use these media outlets responsibly. This policy sets out the principles that St Thomas à Becket School staff are expected to follow.

- Staff should be conscious at all times of the need to keep their personal and professional lives separate. They should not put themselves in a position

where there is a conflict between their work at school, the County Council and personal interests.

- Staff should not engage in activities involving social media which might put St Thomas à Becket School or the County Council into disrepute.

- Staff must not represent their personal views as those of St Thomas à Becket School or the County Council on any social media.

- Staff must not discuss personal info about pupils, St Thomas à Becket School or staff and other professionals you interact with as part of your job on social media.

- Staff must not use social media and the internet in any way to attack, insult, abuse or defame pupils, their family members, colleagues or other professionals St Thomas à Becket School or the County Council.

- Staff must be accurate, fair and transparent when creating or altering online sources of information on behalf of St Thomas a Becket School or the County Council.

- Staff members must not identify themselves as St Thomas à Becket School staff in their personal web space. This is to prevent info on these sites from being linked with the school and the County Council and to safeguard the privacy of staff members.

- Staff members must not have contact through any personal social medium with any pupil from St Thomas à Becket School unless those pupils are family members.

- Staff decline friend requests from pupils on their own personal space.

- Although it is recommended that parents of pupils are not accepted as friends of staff it is recognised in a village community that some staff may be friends with parents of children at the school. School related issues should not be discussed and caution should be taken with any photographs or information that are posted on social media.

- Staff must decline friend requests from pupils (Except family members).

- No photographs of pupils must be published on personal or other websites other than the school website and official school Facebook page.

- Caution is advised when inviting work colleagues to be friends in personal social networking sites.

- Any breach of this policy may lead to disciplinary action being taken against the staff members.

- 2013 St Thomas a Becket webpage authorised contributors: Head teacher, admin office.

- Facebook page authorised administrators: Helen Mockridge (parent who adds diary events/reminders) Head teacher. Comments moderated by head teacher.

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.

Signed: ……

Position: ……..

Date: ……