St Andrew’s CEVA Primary School

E-safety Policy (Acceptable Use) 2018/2019

Background & Rationale

The potential that technology has to impact on the lives of all citizens increases year on year. This is probably even truer for children, who are generally much more open to developing technologies than many adults. In many areas, technology is transforming the way that schools teach and that children learn. At home, technology is changing the way children live and the activities in which they choose to partake; these trends are set to continue.

While developing technology brings many opportunities, it also brings risks and potential dangers of which these are just a few:

- Radicalisation - being drawn into terrorism.
- 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 with 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 videos / internet games.
- An inability to evaluate the quality, 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 social and emotional development and learning.

This policy sets out how we strive to keep children safe with technology while they are in school. We recognise that children are often more at risk when using technology at home (where we have no control over the technical structures we put in place to keep them safe) and so this policy also sets out how we educate children of the potential risks. We also explain how we attempt to inform those people who work with our children beyond the school environment (parents, friends and the wider community) to be aware and to assist in this process.

Policy and leadership

This section begins with an outline of the key people responsible for developing our E-Safety Policy and keeping everyone safe with ICT. It also outlines the core responsibilities of all users of ICT in our school.

It goes on to explain how we maintain our policy and then to outline how we try to remain safe while using different aspects of ICT.

Responsibilities: ICT & e-safety coordinators

Our ICT coordinators along with our ICT technicians, head teacher and governors are responsible for day to day issues.

Their responsibilities include: -

- Taking day to day responsibility for e-safety issues.
- Keeping the e-safety policy up to date.
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an E-safety incident.
- Providing training and advice for staff.
- Liaising with the Local Authority.
- Liaising with school ICT technical staff.

- Receiving reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- Attending training to support e-safety throughout the school.

Responsibilities of teaching staff:-

- Taking day to day responsibility for e-safety issues.
- Have an up to date awareness of e-safety matters and of the current school e-safety policy and practices.
- Report any suspected misuse or problems to the E-Safety Co-ordinator.
- Ensure that E-safety issues are embedded in the curriculum and other school activities.
- Provide a learning environment for thinking and questioning in which children and young people, can raise controversial questions and concerns. Students need opportunities within appropriate subjects, curricula opportunities to express views, seek advice and have questions answered.

Responsibilities: governors

Our governors are responsible for the approval of this policy and for reviewing its effectiveness. This will be carried out by the governors (or a governors' subcommittee) receiving regular information about e-safety incidents and monitoring reports.

A member of the governing body has taken on the role of e-safety governor which involves:

- Monitoring of E-safety incident logs.
- Monitoring of filtering change control logs.
- Monitoring logs of any occasions where the school has used its powers of search and deletion of electronic devices.
- Reporting to relevant Governors committee / meeting.

Responsibilities: head teacher

The head teacher is responsible for ensuring the safety (including E-safety) of members of the school community. The head teacher and another member of the senior management 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.

Responsibilities: ICT technician

The ICT Technician is responsible for ensuring that:

- The school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- Users may only access the school's networks through a properly enforced password protection policy.
- Shortcomings in the infrastructure are reported to the ICT coordinator or head teacher so that appropriate action may be taken.

Policy development, monitoring and review

This E-safety policy will need to be reviewed by: -

- Head teacher / Senior Leaders
- Teachers
- ICT Technical staff
- Governors (especially the E-safety governor)
- Pupils

E-safety education

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. This is particularly important for helping children to stay safe out of school where technical support and filtering may not be available to them.

E-Safety education will be provided in the following ways:

- A planned E-safety programme should be provided as part of computing, PHSE and other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in and out of school. This will be carried out from Year R right through to year 6.

- All children will annually take part in our E-safety programme and will be awarded with a certificate on completion of each unit.

- We use the resources on CEOP's Think U Know site as a basis for our e-safety education- http://www.thinkuknow.co.uk/teachers/resources/ (Hector's World at KS1 and Cyber CafJ at KS2).

- Key E-safety messages should be reinforced through further input via assemblies and pastoral activities as well as informal conversations when the opportunity arises.

- In lessons where internet use is pre-planned, it is best practice that 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.

- Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.

- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making. *Nb. additional duties for schools under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet.*

Acceptable use policy agreement – pupil (KS1)

This is how we stay safe when we use computers:

- I will ask an adult if I want to use the computer
- I will only use activities that an adult says are OK.
- I will take care of the computer and other equipment.
- I will ask for help from an adult if I am not sure what to do or if I think I have done something wrong.
- I will tell an adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer.
- We can go to www.thinkuknow.co.uk for help

Acceptable use policy agreement – pupil (KS2)

I understand that whist I am a member of St. Andrew's CEVA Primary School I must use technology in a responsible way.

For my own personal safety:

- I understand that my use of technology (especially when I use the internet) will, wherever possible be supervised and monitored.
- I understand that my use of the internet will be monitored.
- I will keep my password safe and will not use anyone else's (even with their permission).
- I will keep my own personal information safe as well as that of others.
- I will tell a trusted adult if anything makes me feel uncomfortable or upset when I see it online.

For the safety of others:

- I will not interfere with the way that others use their technology.
- I will be polite and responsible when I communicate with others,

- I will not take or share images of anyone without their permission.

For the safety of the school:

- I will not try to access anything illegal.
- I will not download anything that I do not have the right to use.
- I will only use my own personal ICT kit if I have permission and then I will use it within the agreed rules.
- I will not deliberately bypass any systems designed to keep the school safe (such as filtering of the internet).
- I will tell a responsible person if I find any damage or faults with technology, however this may have happened.
- I will not attempt to install programmes on ICT devices belonging to the school unless I have permission.
- I will only use social networking, gaming and chat through the sites the school allows.

Signed: S Hodson
Reviewed: October 2018
Next Review: September 2019