Stanton Harcourt CE Primary School

E-Safety Policy 2017 - 2018

Background and 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:

- 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 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 of everyone

It is the responsibility of all teachers, TAs and pupils in the school to constantly:

- Review and monitor this e-safety policy.
- Consider any issues relating to school filtering
- Discuss any e-safety issues that have arisen and how they should be dealt with.

Issues that arise are referred to Lucy Duff as e-safety coordinator to pass on to 123ICT for issues with filtering issues and report any safeguarding concerns to the safeguarding officer and the Oxfordshire Safeguarding Children Board (OSCB).

Responsibilities: e-safety coordinator

Our e-safety coordinator is the person responsible to the head teacher and governors for the day to day issues relating to e-safety.
The e-safety coordinator:

- leads discussions about e-safety with the School Council
- 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
- provides training and advice for staff on the teaching of computing
- liaises with the Local Authority
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments

- meets with e-safety governor to discuss current issues, review incident logs and filtering change control logs
- attends relevant meetings and committees of Governing Body
- reports to Senior Leadership Team when relevant
- receives appropriate training and support to fulfil their role effectively
- has responsibility for informing 123ICT, blocking / unblocking internet sites in the school's filtering system, passing on requests for blocking / un blocking to the ICT Helpdesk

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:

- regular meetings with the E-Safety Co-ordinator with an agenda based on:
- 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: Headteacher

The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety is delegated to the E-Safety Co-ordinator

The Headteacher 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 (see flow chart on dealing with e-safety incidents – below and relevant Local Authority HR / disciplinary procedures)

Responsibilities: classroom based staff

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 have read, understood and signed the school's Acceptable Use Policy for staff
- they report any suspected misuse or problem to the E-Safety Co-ordinator
- digital communications with students (email) should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in the curriculum and other school activities.

Responsibilities: ICT technician (123ICT)

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 has been developed by a working group made up of:

- School E-Safety Coordinator
- Head teacher / Senior Leaders
- Teachers
- ICT Technical staff
- Governors (especially the e-safety governor)

Schedule for development / monitoring / review of this policy

The implementation of this e-safety policy will be monitored by the e-safety committee under the direction of the e-safety coordinator.

Monitoring will take place annually.

The governing body will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) annually.

The e-safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be November 2018.

Should serious e-safety incidents take place, the following external persons / agencies should be informed:

- Oxfordshire Safeguarding Children
- Oxford Police

Policy Scope

This policy applies to all members of the school community (including staff, 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.

Acceptable Use Policies

All members of the school community are responsible for using the school ICT systems in accordance with the appropriate acceptable use policy, which they will be expected to sign before being given access to school systems.

Acceptable use policies are provided in Appendix 1 of this policy for:

- Pupils (EYFS + KS1 / KS2)

- Staff (and volunteers)
- Parents / carers (including permissions to use pupil images / work and to use ICT systems)
- Community users of the school's ICT system

Acceptable use policies are revisited and re-signed annually at the start of each school year and amended accordingly in the light of new developments and discussions with the children which take place at the time. Copies are sent home for further discussion with parents.

For children in EYFS and KS1 parents may sign on behalf of their children Staff and volunteers sign when they take up their role in school and in the future if significant changes are made to the policy.

Parents sign once when their child enters the school. The parents' policy also includes permission for use of their child's image (still or moving) by the school, permission for their child to use the schools ICT resources (including the internet) and permission to publish their work.

Induction policies for all members of the school community include this guidance.

Self Evaluation

Evaluation of e-safety is an on-going process and links to other self-evaluation tools used in school in particular to pre Ofsted evaluations along the lines of the Self Evaluation Form (SEF). The views and opinions of all stakeholders (pupils, parent, teachers …) are taken into account as a part of this process.

Signed R Crouch

Date November 2017

Review Date November 2018

Governor agreed