Coton Primary School E-safety Policy: Safeguarding our children

Background to the Policy

The purpose of this policy is to describe the safeguarding measures in place for adults and children in school:

- the ground rules we have developed in school for using the Internet and online technologies
- how these fit into the wider context of our other school policies
- the methods used to protect children from sites containing pornography, racist or politically extreme views and violence.

Ultimately, the responsibility for setting and conveying the standards that children are expected to follow when using technology, media and information resources, is one the school shares with parents and carers. At Coton Primary School, we feel that the most successful approach lies in a combination of site filtering, of supervision and by fostering a responsible attitude in our pupils in partnership with parents.

The development of our safety policy involved:

- The headteacher (Farah McPhee)
- Designated CPs are (Farah McPhee and Anna Hayesmore)
- Computing Subject Leader (Anna Hayesmore)
- PSHCE subject leader (Elly Lark)

It will be available:

- On school website
- Via the office
- In the school staffroom

Rationale

At Coton Primary school we believe that the use of information and communication technologies in schools brings great benefits. To live, learn and work successfully in an increasingly complex and information-rich society, our children must be able to use technology effectively.

The use of these exciting and innovative technology tools in school and at home has been shown to raise educational standards and promote pupil achievement. Yet at the same time we recognise that 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.

While children and young people need support to keep them safe online, the risks associated with the use of technology are not restricted to just them. E-Safety issues can also affect adults who work or are associated with the school. For example school and personal data being entered on web/social networking sites, fraudulent email traps and cyberbullying. It is impossible to eliminate risk completely. It is therefore essential, through good educational provision to manage the risk and deal with any threat to safety.

Teaching and Learning Using Online Technologies

The internet is a part of everyday life for education, business and social interaction.

Benefits of using online technologies in education include:

- Access to world-wide educational resources
- Inclusion in the NEN connecting all UK schools and resources
- Access to experts who would otherwise be unavailable
- Access to anytime, anywhere learning
- Collaboration across schools, networks of schools and services

When using online technologies, it is essential that children understand how to behave in a safe and responsible manner and also how to react when faced with inappropriate content or situations which make them feel uncomfortable. At Coton Primary School we believe that a comprehensive programme of e-safety education is vital for developing our pupils' ability to use technologies safely. This is achieved using a combination of discrete and embedded activities drawn from a selection of appropriate materials (see appendices)

Our programme for e-safety education is evidenced in teachers' planning either as discrete or embedded activities. Members of staff constantly monitor pupils' use of the internet and other technologies and are able to monitor pupils' use of Starz+ communication and publishing tools.

Messages involving "Risks" and "Rules and Responsibilities" are taught and/or reinforced as detailed in the school's AUP (see appendices).

Technology in our School

The school's ICT infrastructure is designed to minimise the risks associated with adult and pupil use of technology. This is provided and maintained by the Local Authority's Education ICT Service.

This helps to ensure that staff and pupils rarely encounter material which is inappropriate or offensive. If / when they do, the school's AUPs and e-safety education programme ensure that they are equipped to deal with any issues in the most appropriate way.

Technologies regularly used by pupils and adult stakeholders include:

Staff:

- ipads
- Laptop PCs
- Cameras
- Desktop PCs

Pupils:

- ipads
- Laptop PCs
- Cameras
- Desktop PCs

Whilst we recognise the benefits of individual pupil logins to our school network, we prefer to use year group logins for ease of access.

All members of staff have individual, password protected logins to the school network and visitors to the school can access part of the network using a generic visitor login and password.

The school's network can either be accessed using a wired or wireless connection. However, the wireless network is encrypted to the standards advised by the Local Authority and the wireless key is kept securely by the school office. Pupils are **not** permitted to connect personal devices to the school's wireless network.

Safeguarding Our Children Online

Coton Primary School recognises that different users will be expected to use the school's technology systems in different ways – appropriate to their age or role in school. We acknowledge the need to: *Equip children to deal with exposure to harmful and inappropriate content and contact, and equip parents to help their children deal with these things and parent effectively around incidences of harmful and inappropriate conduct by their children. UKCCIS – June 2008*

The school has published Acceptable Use Policies for pupils and staff and all of these stakeholders sign to indicate their acceptance of our AUPs and relevant sanctions which will be applied should rules be broken. (See appendix for AUPs)

Any known or suspicious online misuse or problem will be reported to the designated E-Safety Leader for investigation/ action/ sanctions. The school will keep evidence and/or contribute to a log of any 'extreme' or 'unusual' actions that a pupil has been involved in online. This log will be used to keep track of the child's behaviours over the entire time they are at the school and will be stored alongside other incident logs. These are stored securely by the head teacher.

Responding to Incidents

It is important that all members of staff – teaching and non-teaching – are aware of how to respond if an e-safety incident occurs or they suspect a child is at risk through their use of technology. Responding to an e-safety incident in school is no different to responding to other incidents in school.

If an e-safety incident occurs Coton Primary will follow its usual procedures for dealing with other incidents including internal sanctions and involvement of parents (for ICT, this may include the deactivation of accounts or restricted access to systems as per the school's AUPs – see appendix). Where the school suspects that an incident may constitute a safeguarding issue, the usual Child Protection procedures will be followed: (Also see Child Protection Policy for more details)

Dealing with Incidents and Seeking Help
If a concern is raised, refer immediately to the designated person for child protection. If that is not possible refer to the headteacher or, if necessary, the Chair of Governors.
It is their responsibility to:

Step 1: Identify who is involved – any combination of child victim, child instigator, staff victim, or staff instigator
Step 2: Establish the kind of activity involved and whether it is illegal or inappropriate. If you are in doubt consult the DP or Education Child Protection Service helpline.
Step 3: Ensure that the incident is documented using the standard child protection incident logging form (see appendix)

Depending on the judgements made at steps 1 and 2, the following actions should be taken:

Staff instigator – follow the standard procedures for Managing Allegations against a member of staff. If unsure seek advice from the Local Authority Designated Officer or Education Officer.

Staff victim – Seek advice from your HR provider and/or Educational Child Protection Service

Illegal activity involving a child – refer directly to Cambridgeshire Constabulary – 0845 456 4564 – make clear that it is a child protection issue

Inappropriate activity involving a child – follow standard child protection procedures. If unsure seek advice from Education Child Protection Service helpline: 01223 712096

Education Child Protection Service – June 2010

Equally, if the incident involves or leads to an allegation against a member of staff, the school will follow the usual procedures for dealing with any allegation against a member of staff. (See Whistle Blowing Policy)

This policy was ratified by the governing body on 3rd June 2015.
It will be reviewed annually, in June 2016.

Signed by the head teacher …….

Chair of Governors ……

Terms used in this policy

AUP: Acceptable Use Policy.
A document detailing the way in which new or emerging technologies may/may not be used – may also list sanctions for misuse.

Child: Where we use the term 'child' (or its derivatives), we mean 'child or young person'; that is anyone who has not yet reached their eighteenth birthday.

E-safety: We use e-safety, and related terms such as 'online', 'communication technologies', and 'digital technologies' to refer to all fixed and mobile technologies that children may encounter, now and in the future, which might pose e-safety risks. We try to avoid using the term 'ICT' when talking about e-safety as this implies that it is a technical issue – which is not the case. The primary focus of e-safety is child protection: the issues should never be passed solely to technical staff to address.

PIES: A model for limiting e-safety risks based on a combined approach to policies, infrastructure and education, underpinned by standards and inspection.
Safeguarding: Safeguarding is defined (for the purposes of this document) as the process of increasing resilience to risks when using technology through a combined approach to policies and procedures, infrastructure and education, underpinned by standards and inspection. E-safety is just one aspect of a much wider safeguarding agenda within the UK, under the banner of *Every Child Matters: Change for Children*. Those with responsibility for the development and delivery of e-safety policies should embed their work within the wider safeguarding agenda, and work across services to ensure that they are delivering the best possible opportunities for the children and young people in their care.

Schools: For ease of reading we refer predominantly to schools within this publication, but the underlying principles can be applied equally to any setting with responsibility for educating or safeguarding children and young people.

Users: We use this term, and related terms such as service users and end users, to mean those people who will ultimately be bound by the provisions of an

AUP – this might be pupils, staff, parents and carers, or members of the wider community, depending on provisions of your AUP or the context in which you operate.

Appendix: AUPs- pupil, staff

KS1 ICT Agreement

- I will only use the school's ICT equipment and tools for school tasks.
- I will only use the internet and email when an adult is nearby.
- I will keep my passwords 'Top Secret' and tell my teacher if I think someone else knows them.
- I will only use my school e-mail address when e-mailing.
- I will ask an adult before opening an email from someone I don't know.
- I will not share details about myself such as surname, phone number or home address.
- I will ask if I need to look at other peoples' work on the computer.
- I will only send friendly and polite messages.
- I will ask my teacher before using photos or video.
- If I see something on a screen which upsets me, I will always tell an adult.

My name: ……..

Date: ……..

Starz E-Safety Rules

I use Starz+ to help me to stay safe online

I will keep my Starz password TOP SECRET and tell my teacher if someone else knows it.

I only click on the buttons or links when I know what they do.

In school I use Starz to search the Internet because it keeps me safe.

If I see something on a screen which upsets me, I will always tell an adult.

I will send only polite and friendly emails to people that I know using Starz mail.

I will only put polite and friendly things online.

(Sample poster to display in KS1 classrooms)

KS2 ICT Agreement

- I will use the school's ICT equipment and tools respectfully, and only for school tasks.
- I will only use the Internet if a teacher or teaching assistant is supervising me.
- I will only delete my own files unless my teacher gives me permission to delete someone else's. I will not look at other people's files without their permission.
- I will keep my passwords secret and tell my teacher if I think someone else knows them.
- I will only use my class e-mail address or my own school e-mail address when e-mailing at school.
- I will only open e-mail attachments from people who I know or my teacher has approved. If I am unsure about an attachment or e-mail, I will ask my teacher for help.
- I will make sure that all communication with other children and adults is responsible, polite and sensible.
- I will not give my own personal details such as surname, phone number or home address or any other personal details that could be used to identify me, my friends or my family. If I have to use an online name I will make one up!
- I will never post photographs or video clips of people I know without permission and never include names with photographs or videos.
- I will never arrange to meet someone I have only ever previously met online. It could be dangerous.
- I will not deliberately look for, save or send anything that could be unpleasant or upsetting. If I find anything via Internet, e-mail or mobile phone that is upsetting or makes me feel uncomfortable, I will tell a teacher or responsible adult.
- I will not use mobile phones on school grounds during the school day.
- I will be responsible for my behaviour because I know that these rules are there to keep me safe. If I break these rules then I may be stopped from using the computers in school, removed from Starz+ and my parents may be informed.

Signed: .....

Date: .....

Coton School Staff Acceptable Use Policy

I agree and accept that any computer or laptop loaned to me by the school is provided solely to support my professional responsibilities. I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's management information system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority. I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.

I will

- only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- use the approved, secure email system(s) for all school business.
- only communicate with parents/carers for appropriate school business using the office e-mail account.
- ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- report any accidental access to, or receipt of inappropriate materials, or filtering breach to the e-Safety Co-ordinator, Designated Person for Child Protection or Headteacher, as appropriate
- use the school's Learning Platform in accordance with school and Local Authority advice.
- ensure that any out-of-work, private social networking sites / blogs etc that I create or actively contribute to do not compromise and are not confused with my professional role, and do not bring Coton school into disrepute.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- will promote e-safety with pupils in my care and will help them to develop a responsible attitude to their use of ICT.
- follow the school policy on the use of mobile phones and cameras.

I will not

- share or reveal my password(s) to anyone.
- allow unauthorised individuals to access email / Internet / intranet / network, or other school / LA systems.
- engage in any online activity that may compromise my professional responsibilities
- allow children to logon using my username and password
- browse, download or send material that could be considered offensive, illegal or discriminatory.
- download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software.
- use personal digital cameras or mobile phones for taking and transferring images of pupils or staff.
- I will not store images at home.

I understand that once I sign this document, failure to comply with this agreement could lead to disciplinary action.

Name: **Signed:** **Date:**