Caldecote Primary School

Online Safety Policy: Safeguarding our children

January 2019

1. 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 Caldecote Primary School, we feel that the most successful approach lies in a combination of site filtering, of supervision and by fostering a responsible attitude with our pupils in partnership with parents.

2. Rationale

At Caldecote 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. Online 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 cyber bullying. 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.

3. 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
- 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 Caldecote Primary School we believe that a comprehensive programme of online 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.

Our programme for online 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). Parents have all signed the Home / School agreement consenting to "support the schools' policies and guidelines" which give guidance and advice on safe internet use.

4. 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 both E2BN and 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 online 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:

Use of hand held technology (personal phones and hand held devices)
We recognise that the area of mobile technology is rapidly advancing and it is our school's policy to review its stance on such technology on a regular basis. Currently our policy is:

- Members of staff are permitted to bring their personal mobile devices into school and must abide by the school's Mobile Device Policy and Mobile Phone Guidance.
- Pupils are not currently permitted to bring their personal hand held devices into school.

Email
Access to email is provided for all users in school via the intranet page accessible via the browser (Internet Explorer) from their laptops.

These official school email services may be regarded as safe and secure and are monitored.

- Staff should only use the school email services to communicate with others for all school business
- Users need to be aware that email conversations may be monitored.
- Pupils have access to an individual email account (via Starz+) for communication with pupils registered at school. These emails are closely monitored by staff.
- A structured education programme is delivered to pupils which helps them to be aware of the dangers of and good practises associated with the use of emails.

Use of digital and video images

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing images
- Members of staff are allowed to take digital still images and video images to support educational aims, but must follow school policies concerning sharing, distribution and publication of those images.

- Care should be taken when taking digital / video images that pupils are appropriately dressed.
- Pupils must not take, use, share, publish or distribute images of others without their permission.

Use of web-based publication tools

Our school uses the public facing website http://www.caldecoteprimaryschool.org.uk and a school Twitter account for sharing information with the community beyond our school. This includes celebrating work and achievements of children. All users are required to consider good practise when publishing content.

- Personal Information should not be posted and only official email addresses provided as links.
- Only pupils' first names are used and only when necessary.
- Photographs published that include pupils will be selected carefully and will comply with the following good practice guidance on the use of such images:
    - Pupils' full names will not be used anywhere and never in association with photographs.
    - Written permission from parents or carers will be obtained before photographs of pupils are published on the school website. Consent is obtained via the school Permissions form when children first register.

Virtual Learning Environment (VLE) Starz+

Class teachers monitor the use of the VLE regularly, but with particular attention to messaging and communicating.

Staff use is monitored by the administrator (ICT leader).

User accounts and access rights can only be created by the school administrator and LA administrators.

Pupils are required to sign a safe user agreement before using the VLE.

Only current members on the school register will have access to the VLE.

When staff, pupils, etc leave the school their accounts or rights to specific school areas will be disabled.

Any concerns with content may be recorded and dealt with in the following ways;

a) The user will be asked to remove any material deemed inappropriate or offensive.
b) The material will be removed by the site administrator if the user does not comply.
c) Access to the VLE for the user may be suspended.
d) The user will need to discuss the issue with a member of the SLT before reinstatement.
e) A pupil's parent/carer may be informed.

Professional standards for staff communication

In all aspects of their work in our school teachers abide by the Teachers' Standards as described by the DfE https://www.gov.uk/government/publications/teachers-standards Teachers apply these standards appropriately for all matters relating to online safety.

Any digital communication between staff and pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content.

- These communications may only take place on official (monitored) school systems.
- Personal email addresses, text messaging or public chat / social networking technology must not be used for these communications.

Filtering

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide 100% guarantee that it will do so. As a school buying broadband services from Cambridgeshire ICT Services we automatically receive the benefits of a managed filtering service, with some flexibility for changes at local level.

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 be accessed using either a wired or wireless network. Wireless is encrypted to the standards advised by the Local Authority and the key is kept securely by the school office. Pupils are **not** permitted to connect personal devices to the school's wireless network unless they have permission from the ICT leader.

5. Safeguarding Our Children Online

Caldecote 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:

The school has published Acceptable Use Policies for pupils, staff and parents (on their Permissions form) and all of these stakeholders sign to indicate their acceptance of our AUPs

and relevant sanctions which will be applied should rules be broken. These are available on the website or from the school office.

The following is a summary of some of the key messages held within our AUPs. Please see appendices for full details.

Any known or suspicious online misuse or problem will be reported to the designated Online safety leaderfor 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 Headteacher.

6. **Responding to Incidents**

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

If an online safety incident occurs Caldecote 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 Safeguarding procedures will be followed:

Dealing with Incidents and Seeking Help
If a concern is raised, refer immediately to the designated persons for child protection. If that is not possible and it is an emergency, either contact the Educational Safeguarding team or Mrs. Sarah Jarman (Headteacher, Monkfield Primary School).
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 Education Safeguarding advice line
Step 3: Ensure that the incident is documented using the standard Logging a Concern form (green)

Depending on the judgements made at steps 1 and 2 the following actions may 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 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 Safeguarding advice line
Extremist or Cultural concerns – refer to the School Prevent leader

Equally, if the incident involves or leads to an allegation against a member of staff, the school will follow the procedures for dealing with any allegation against a member of staff (see appendix).

7. 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. The Acceptable User 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.

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.

Online safety: We use online 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 online safety risks. We try to avoid using the term 'ICT' when talking about online safety as this implies that it is a technical issue – which is not the case. The primary focus of online safety is child protection: the issues should never be passed solely to technical staff to address.

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. Online 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 online 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 policy, but the underlying principles can be applied equally to any setting with responsibility for educating or safeguarding children and young people.

SLT: Senior Leadership Team (Headteacher, Deputy Headteacher, Key Stage 1 & 2 Leaders & SENCo)

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

8. Appendices: which should be read alongside this policy

- Acceptable Internet Use Policy
- Allegations of Abuse Against Staff Policy
- Appropriate Use of Staff Laptops Policy
- Data Protection Policy
- Confidentiality Policy
- Mobile Device Policy
- Safeguarding & Child Protection Policy
- Social Networking Policy
- Whistleblowing Policy
- Anti-Bullying Policy
- Computing Policy
- Safer User Agreements
- Acceptable Use Policy
- PSHE Policy
- Home School Agreement
- School Permissions
- Keeping Children Safe in Education