

# Clipston Endowed VC Primary School

## Online Safety Policy



### Online Safety Policy

*In this policy, the role of the governor states that they are responsible for ensuring the effective implementation, monitoring and evaluation of the policy. This - in practical terms - means that this is a day to day management responsibility usually overseen by the Head Teacher, and governors receive a report on the effectiveness of the policy when a policy is reviewed.*

**This policy should be read in conjunction with the Remote Education Policy**

Adopted by the Governing Body: Autumn 2020

Proposed Review: Autumn 2021

Signed .....

Mrs Helen Bellamy - Chair of Governors

## **AIMS OF CLIPSTON SCHOOL**

Clipston Endowed VC Primary School aims to provide every child with high quality teaching and learning. It is the school's philosophy to give our pupils a measure of independence, a high level of self-confidence, a deep sense of self-worth, and an understanding and deeper appreciation of our Christian heritage. To achieve this, we aim to:

- a) Enable all children to achieve their full potential, both academically, socially, personally, and morally in order that children expect the best of themselves.
- b) Promote spiritual development and the ability to grow and flourish as human beings.
- c) Support children in building relationships which reflect Christian values.
- d) Deliver a broad, relevant and challenging education which is of a high standard and appropriate to an individual child's needs.
- e) Promote high standards of behaviour based on mutual trust and respect, developing responsibility and fostering self-discipline.
- f) Promote good citizenship, thus enabling individuals to make valuable contributions to wider society.
- g) Ensure equal opportunities for all.
- h) Provide a welcoming and stimulating learning environment in which everyone feels safe, happy and secure.
- i) Develop a sense of pride in belonging to Clipston Endowed VC Primary School.

To achieve these aims staff and governors will work in partnership with parents, carers and the local community for the benefit of all our pupils.

## **ON-LINE BENEFITS AND RISKS**

Computing covers a wide range of activities, including access to information, electronic communications and social networking. As use of technology is now universal, it is imperative that children learn computing skills in order to prepare themselves for their future learning and working environment, and that the inherent on-line risks are not used to reduce the use of technology by pupils. This document provides guidance on developing an effective on-line safety strategy to ensure that staff recognise the risks and take action to help children use the internet safely and responsibly.

## **COMPUTING IN OUR SCHOOL.**

Computing is a key part of the school curriculum and one of the key aims of computing is to ensure that pupils are aware of on-line safety messages and guidelines that we continue to teach and instill in our pupils. This is part of our school's responsibility to safeguard and promote the welfare of our pupils, as well as the duty of care to children and their parents to provide a safe learning environment.

Clipston Primary School's online safety strategy is based on a framework of policy and practice with educational and technological support that ensures an on-line learning environment that maximises the educational benefits of IT whilst minimising the associated risks.

Our purpose is to:

- a) promote the use of technology within the curriculum;
- b) protect children from harm;
- c) safeguard staff in their contact with pupils and their own use of the internet;
- d) ensure the school fulfils its duty of care to pupils;
- e) provide clear expectations for staff and pupils on acceptable use of the internet.

In particular, we ensure the following:

- A **safe internet procedure that** provides filtering software to block access to unsuitable sites, anti-virus software and monitoring systems (for example Surfprotect).
- A culture of **safe practice** underpinned by a strong framework of on-line safety processes that ensures everyone is aware of expected standards of on-line behaviour.
- Children are **taught to keep themselves and others safe** on-line and use technology responsibly; this should be achieved by working in partnership with parents and carers and raising awareness of the potential risks of internet use.

## **ROLES AND RESPONSIBILITIES**

A successful online safety strategy needs to be inclusive of the whole school community, including teaching assistants, governors and others, and forge links with parents and carers.

**Mrs Mercer has ultimate responsibility for all on-line safety issues within the school including:**

- the overall development and implementation of the school's on-line safety policy;
- ensuring that on-line safety issues are given a high profile within the school community;
- linking with parents and carers to promote on-line safety;
- ensuring on-line safety is embedded in the curriculum;

### **Governor roles**

Governing bodies have a statutory responsibility for pupil safety and should therefore be aware of on-line safety issues, providing support to the head teacher in the development of the school's on-line safety policy.

### **On-line safety/Computing coordinator's role**

All schools should have a designated on-line safety coordinator who is responsible for co-ordinating on-line safety procedures on behalf of the school.

This person is: **Miss Steph Glascodine**

### **Role of school staff**

All school staff have a dual role concerning their own internet use and providing guidance, support and supervision for pupils. Their role is to:

- adhere to the school's on-line safety policy and procedures;
- communicate the school's on-line safety policy to pupils;

- keep pupils safe and ensure they receive appropriate supervision and support whilst using the internet;
- report breaches of internet use to the on-line safety coordinator / Headteacher;
- teach the on-line safety and digital literacy elements of the National Curriculum.

### **WORKING WITH PARENTS AND CARERS**

Most children will have internet access at home or own mobile devices and might not be as closely supervised in its use as they would be at school. Therefore, parents and carers need to know about the risks so that they are able to provide on-line safety education at home and regulate and supervise children's use as appropriate to their age and understanding.

From time to time, parents are made aware of on-line safety issues and are offered support in reinforcing online safety messages at home.

### **TEACHING ON-LINE SAFETY**

One of the key features of our school's online safety strategy is teaching pupils to protect themselves and behave responsibly while on-line.

- Overall responsibility for the design and co-ordination of on-line safety education lies with the head teacher and the on-line safety coordinator but all staff should play a role in delivering on-line safety messages.
- Teachers are primarily responsible for delivering an ongoing on-line safety education in the classroom as part of the curriculum.
- The start of every lesson where computers are being used should be an opportunity to remind pupils of expectations on internet use and the need to follow basic principles in order to keep safe.
- Teachers should be aware of those children who may be more vulnerable to risk from internet use, generally those children with a high level of experience and good computer skills but coupled with poor or under-developed social skills.

### **Content**

Pupils should be taught all elements of on-line safety included in the computing curriculum so that they can use technology safely and respectfully, keeping personal information private and identify where to go for help and support when they have concerns about content or contact on the internet or other on-line technologies.

Ultimately, we aspire to our pupils being responsible, competent, confident and creative users of information and communication technology.

### **IT and safe practice**

School staff need to be aware of the importance of maintaining professional standards of behaviour with regards to their own internet use, particularly in relation to their communications with pupils.

Adults in school are required to abide by the **Adult Code of Conduct**.

## **SAFE USE OF TECHNOLOGY**

### **Internet and search engines**

- When using the internet, children should receive the appropriate level of supervision for their age and understanding. Teachers should be aware that often, the most computer-literate children are the ones who are most at risk.
- Pupils should not be allowed to aimlessly “surf” the internet and all use should have a clearly defined educational purpose.
- Despite filtering systems, it is still possible for pupils to inadvertently access unsuitable websites. Systems are in place to report, log and act upon these incidents.

### **Safe use of applications**

Our school has identified a clear educational use for certain social networking sites (e.g. Twitter). These approved sites are used to inform parents and carers of news and events.

- Pupils should be taught to be wary of opening attachments to emails where they are unsure of the content or have no knowledge of the sender.
- Pupils should be taught not to disclose personal contact details for themselves or others such as addresses or telephone numbers via email correspondence or on social networking sites.
- Pupils should be warned that any bullying or harassment via email, chat rooms or social networking sites will not be tolerated and will be dealt with in accordance with the school’s anti-bullying policy. This should include any correspondence or contact taking place outside the school and/or using non-school systems or equipment.
- In order to teach pupils to stay safe on-line inside and outside of school, they are taught to follow our schools on-line safety guidelines:
  - a) To seek the help of an adult if they see or do something on-line that worries them;
  - b) not to give out personal details to anyone on-line that may help to identify or locate them or anyone else, for example home address, name of school or clubs attended;
  - c) to think carefully before uploading personal photos of themselves or others onto sites and to take care regarding what information is posted as the images will be owned by the site and therefore there is no control where images may end up or who can see them;
  - d) to behave responsibly whilst on-line and keep communications polite;
  - e) not to respond to any hurtful or distressing messages but to let their teachers, parents or carers know so that appropriate action can be taken;
  - f) not to arrange to meet anyone whom they have only met on-line.

### **SCHOOL WEBSITE**

Mrs Jan Heaney is our school’s designated person to have responsibility for uploading materials onto the school websites.

- We ensure the privacy and security of staff and pupils, the contact details on the website should be the school address, email and telephone number. No contact details for staff or pupils should be contained on the website.
- Children’s full names should not be published on the website.
- Links to any external websites are regularly reviewed to ensure that their content is appropriate for the school and the intended audience.

## **PHOTOGRAPHS AND VIDEO IMAGES**

- Children's names are not published where their photograph can be linked directly to their name, except on the Tapestry secure site, which is personal to each child and only accessed by the parent (and shared by others only approved by them).
- Staff should ensure that children and staff are suitably dressed to reduce the risk of inappropriate use of images.

## **RESPONDING TO INCIDENTS**

- All incidents and complaints relating to on-line safety and unacceptable internet use will be reported to Mrs Mercer.
- Incidents involving the head teacher should be reported to the chair of the board of governors.
- The school will keep a log of all on-line safety / computing incidents and complaints. Governors will regularly review the information for evidence of emerging patterns of individual behaviour or weaknesses in the school's on-line safety system, and use these to update the on-line safety policy.

## **CYBERBULLYING**

### **Definition and description**

Cyberbullying is defined as the use of technology such as email and social networking sites to deliberately hurt or upset someone or harass or threaten. Unlike physical forms of bullying, the internet allows bullying to continue past school hours and invades the victim's home life and personal space. It also allows distribution of hurtful comments and material to a wide audience.

Cyberbullying is extremely prevalent as people who would not consider bullying in the physical sense may find it easier to bully through the internet, especially if it is thought the bullying may remain anonymous.

Bullying may take the form of:

- Continued rude, abusive or threatening messages via email or text;
- posting insulting, derogatory or defamatory statements on blogs or social networking sites;
- setting up websites that specifically target the victim;
- making or sharing derogatory or embarrassing images or videos of someone via mobile phone or email or social networking platforms.

Cyberbullying can affect pupils, parents and staff members. Often, the internet medium used to perpetrate the bullying allows the bully to remain anonymous.

### **Dealing with incidents**

The school's Anti-Bullying Policy covers all incidents of bullying that involve pupils and staff at school, whether or not they take place on school premises or outside school.

-~--~-