

# Esafety Policy



Created: September 2017  
Review: September 2018

## 1. Introduction

New technology is being created on an almost daily basis and is now an integral part of life for both adults and children alike. These are powerful tools, which when used properly, can open up new opportunities for everyone. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

We are required to ensure that children learn how to use these technologies safely and have access to safe internet at all times. This is addressed as part of a wider duty of care to which all who work in schools are bound.

## 2. Potential Risks

However, 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.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

## 3. Policy Statements

### **Education:** Pupils

Pupils will follow a purchased scheme of work which incorporates e-safety at appropriate times. (See Curriculum) This will be built on year on year to ensure pupils have a secure understanding of how to stay safe online.

## **Education:** Parents / Carers

Parents and carers are offered regular internet safety sessions. They can find further guidance from [here](#).

## **Education and training:** Staff and Governors

Staff and governors are given training about e-safety every year. They can also seek advice when necessary from the e-Safety Officer.

## **Monitoring and Filtering**

- The school uses a filtering system provided by [swgfl.org.uk](http://swgfl.org.uk). This blocks unsuitable content to ensure that pupils view only web pages suitable for them. Any filtering issues are reported immediately to SWGFL.
- The school system is securely located within a locked room that only a few members of staff have access to.
- Master and administrator passwords are securely stored and are only available to limited staff.
- Users are responsible for protecting their usernames and passwords
- All members of the school have clearly defined access rights which are decided by their role within school.
- Passwords are changed regularly.
- The school system is protected by anti-virus software, which is updated regularly.

## **Curriculum**

Pupils will learn:

### **Year 1:**

- To let an adult know if they are worried about an image.
- That there are some pictures they can copy and some that they can't.
- That they shouldn't put their name or a photo of themselves on the web.

### **Year 2** (plus a recap of previous learning):

- To tell someone if they are worried about a computer game.
- That some games are for older children.
- That it can be hard to stop playing computer games.
- That there are some photos that shouldn't put on the web.
- To check if an email and an attachment are from someone they know and trust.
- What to do if they are worried about opening an email.
- To be careful about opening emails and attachments.

### **Year 3** (plus a recap of previous learning):

- What to do if they have concerns about things on the internet at school.
- What to do if they have concerns about things on the internet at home.
- To follow the school's rules and use email and video conferencing safely.
- That it is important to keep all personal data private.

### **Year 4** (plus a recap of previous learning):

- To be safe and responsible when creating a web page.

#### **Year 5** (plus a recap of previous learning):

- How important it is to keep passwords secret.
- To create a secure, hard-to-guess password.
- To check the security certificates for a web page.
- To use blogs safely and responsibly.

#### **Year 6** (plus a recap of previous learning):

- That there are some photos that shouldn't put on the web and that these images cannot be totally removed once uploaded.
- About [sexting](#) and how this may impact on them.

### **Use of digital and video images - Photographic, Video**

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate parents about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment. The personal equipment of staff should not be used for such purposes.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Parents will be asked to sign an agreement at the start of each academic year.

### **Data Protection**

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed

- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- The data must be encrypted and password protected.
- The device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected).
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

## **Communications**

The school understands that many young people have access to a range of mobile technology. However, children are actively discouraged from bringing these into school as all communication should be through the office. The exception to this is year six children who walk home by themselves. In these cases, children are expected to hand their mobile device in to the school office. Pupils are not allowed to use their own mobile devices in school for any reason.

- All 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 via the office administration account. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications.
- Class email addresses will be used in both KS1 and KS2, for whole class communication.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

## **Responding to incidents of misuse**

In school, SWGFL should filter all content that is inappropriate, however, in very rare circumstances; pupils may see something they are unhappy about. If this happens a



pupil should click on Hector the Protector and tell an adult immediately. SWGFL will be informed of these immediately.

If a parent is unhappy about something that occurred outside school, the child's teacher should be informed of anything that may affect them. Parents may also feel it necessary to contact other agencies such as [CEOP](#).

#### **4. Roles and Responsibilities**

The teaching of e-safety and this policy is checked and overseen by governors, the head teacher, senior leaders and the e-safety officer.

Teaching staff are responsible for the safe use of computers within the classroom and the day to day teaching of e-safety, ensuring that pupils follow instructions precisely and using the behaviour system appropriately when necessary.

Pupils are expected to follow the SMART rules outlined [here](#).

Parents and carers play a crucial role in ensuring that their children understand the need to stay safe online. It is important that a family agreement is considered. A family agreement is a great way to start a conversation with the whole family about how everyone uses the internet, and discuss together how to behave in a positive way when online at home, at school, at friend's houses etc. An example of one can be found [here](#). This can be downloaded and printed for use at home.

# Pupil Acceptable Use Policy Agreement

**(All Pupils)**

**This is how we stay safe when we use computers:**

- I will ask a teacher or suitable adult if I want to use the computers
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will take care of the computer and other equipment
- I will ask for help from a peer, teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or suitable 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.

Signed (child):.....(Year 2 and above)

Signed (parent): .....

Date: .....

## Parental Permission Form 2017/18

### Internet Use

- Calton Primary School has a high speed Broadband connection which allows children fast access to the Internet for use across the curriculum including the Computing Curriculum.
- We ask your permission to allow your child to use the Internet, e-mail, class blogs and participate in all internet related activities. Your child's Internet access will be fully supervised at all time and we can assure you that the school has set up filters to restrict access to known sites that may not be suitable for children.

### Digital Media

- Digital Learning is an integral part of your child's education and we regularly use digital media to video or photograph the children's learning experiences. These images may be used in our school's prospectus and other printed material, on our website as well as on social media sites such as Twitter and class blogs. Images will not identify your child by name and will be used in conjunction with our E-Safety policy.
- From time to time, our school may be visited by the media who will take photographs or film footage of events. Pupils will often appear in these images, which may appear in local or national newspapers, or in televised news programmes or on social media sites.
- To comply with the Data Protection Act 1998, we need your permission before we can photograph or make any recordings of your child. Please sign giving your permission and return this form to school.

### Internet and digital media Permission Form

I do/do not grant permission for my child to use electronic mail and the Internet.

(delete as appropriate)

I do/do not agree to my child using digital media technologies to enhance their learning. (delete as appropriate)

☐

I understand that the school has set up filters to restrict access to known sites that may not be suitable for children, however, pupils should take responsibility for their own actions. I understand that some material on the Internet may be objectionable and I accept responsibility for setting standards for my child to follow when selecting, sharing and exploring information and media.



## **Useful Links**

Child Exploitation and Online Protection Centre (CEOP)

- <http://www.ceop.gov.uk/>

ThinkUKnow

- <http://www.thinkuknow.co.uk/>

Childnet International:

- [www.childnet.com](http://www.childnet.com)
- [www.childnet.com/parents-and-carers](http://www.childnet.com/parents-and-carers)
- [www.childnet.com/resources/supporting-young-people-online](http://www.childnet.com/resources/supporting-young-people-online)
- [www.childnet.com/sns](http://www.childnet.com/sns)
- [www.childnet.com/parents-help](http://www.childnet.com/parents-help)
- [www.childnet.com/have-a-conversation](http://www.childnet.com/have-a-conversation)

UK Safer Internet Centre:

- [www.saferinternet.org.uk/parents](http://www.saferinternet.org.uk/parents)
- [www.saferinternet.org.uk/parent-tech](http://www.saferinternet.org.uk/parent-tech)
- [www.saferinternet.org.uk/parental-controls](http://www.saferinternet.org.uk/parental-controls)
- [www.saferinternet.org.uk/safety-tools](http://www.saferinternet.org.uk/safety-tools)
- [www.saferinternet.org.uk/checklists](http://www.saferinternet.org.uk/checklists)

KidSMART

- [www.kidsmart.org.uk](http://www.kidsmart.org.uk)

PhoneBrain

- [www.phonebrain.org.uk](http://www.phonebrain.org.uk)

Ask About Games

- [www.askaboutgames.com](http://www.askaboutgames.com)

NetAware

- [www.net-aware.org.uk](http://www.net-aware.org.uk)

Common Sense Media

- [www.commonsensemedia.org](http://www.commonsensemedia.org)

## Digital Parenting

- [www.vodafone.com/content/parents](http://www.vodafone.com/content/parents)

## Internet Matters

- [www.internetmatters.org](http://www.internetmatters.org)

## Childline

- [www.childline.org.uk](http://www.childline.org.uk)

BBC Chatguides: <http://www.bbc.co.uk/chatguide/index.shtml>

Kidsmart: <http://www.kidsmart.org.uk/default.aspx>

Know It All - <http://www.childnet-int.org/kia/>

Cybersmart - <http://www.cybersmartcurriculum.org/home/>

NCH - <http://www.stoptextbully.com/>

Chatdanger - <http://www.chatdanger.com/>

Internet Watch Foundation: <http://www.iwf.org.uk/media/literature.htm>

Digizen – cyber-bullying films: <http://www.digizen.org/cyberbullying/film.aspx>

London Grid for Learning: <http://cms.lgfl.net/web/lgfl/safety/resources>



## Useful terms

CEOP Child Exploitation and Online Protection Centre (part of UK Police)

DFE Department for Education

ICT Information and Communications Technology

KS1/ KS2 Key Stage 1 2 – schools are structured within these multiple age groups  
eg KS2 = years 3 to 6 (age 7 to 11)

LA Local Authority

LAN Local Area Network

Ofsted Office for Standards in Education, Children's Services and Skills

PHSE Personal, Health and Social Education

SWGfL South West Grid for Learning – the Regional Broadband Consortium of  
SW Local Authorities – is the provider of broadband and other services  
for schools and other organisations in the SW

VLE Virtual Learning Environment (a software system designed to support  
teaching and learning in an educational setting,

WAP Wireless Application Protocol

Sometimes children use acronyms which we do not understand. This link will give you  
a list of those currently used:

[http://www.safesurfingkids.com/chat\\_room\\_internet\\_acronyms.htm](http://www.safesurfingkids.com/chat_room_internet_acronyms.htm)