



---

# On-Line Safety Policy

Date: September 2021

Due for Review: September 2023

---

Online safety is part of the school's safeguarding responsibilities. This policy relates to other policies including those for **behaviour, safeguarding, anti-bullying, data handling and the use of images.**

## Using this policy

- The school will form an online safety committee and will appoint an online safety co-ordinator.
- Our online safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior management and approved by governors.
- The online safety policy was revised by Jo Hastings
- It was initially approved by the Governors on: 10<sup>th</sup> March 2016
- The online safety policy and its implementation will be reviewed annually. The next review is due in September 2021
- The online safety policy covers the use of all technology which can access the school network and the internet or which facilitates electronic communication from school to beyond the bounds of the school site. This includes but is not limited to workstations, laptops, mobile phones, tablets and hand held games consoles used on the school site.
- The online safety policy recognises that there are differences between the use of technology as a private individual and as a member of staff / pupil.

## Managing access and security

The school will provide managed internet access to its staff and pupils in order to help pupils to learn how to assess and manage risk, to gain the knowledge and understanding to keep themselves safe when using the internet and to bridge the gap between school IT systems and the more open systems outside school

- The school will use a recognised internet service provider or regional broadband consortium.
- The school will ensure that all internet access has age appropriate filtering provided by a recognised filtering system which is regularly checked to ensure that it is working, effective and reasonable.
- The school will ensure that its networks have virus and anti-spam protection.
- Access to school networks will be controlled by **personal** passwords.
- Systems will be in place to ensure that internet use can be monitored and a log of any incidents will be kept to help to identify patterns of behaviour and to inform online safety policy.
- The security of school IT systems will be reviewed regularly.
- All staff that manage filtering systems or monitor IT use will be supervised by senior management and have clear procedures for reporting issues.
- The school will ensure that access to the internet via school equipment for anyone not employed by the school is filtered and monitored.

## **Internet Use**

The school will provide an age-appropriate online safety curriculum that teaches pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety.

All communication between staff and pupils or families will take place using school equipment and/or school accounts.

## **Pupils will be advised not to give out personal details or information which may identify them or their location**

### **E-mail**

- Pupils and staff may only use approved e-mail accounts on the school IT systems.
- Staff to pupil email communication must only take place via a school email address or from within the learning platform.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school will consider how e-mail from pupils to external bodies is presented and controlled.

### **Published content eg school web site, school social media accounts**

- The contact details will be the school address, email and telephone number. Staff or pupils' personal information will not be published.
- The head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

### **Publishing pupils' images and work**

- Written permission will be obtained from parents or carers before photographs or names of pupils are published on the school web site or any school run social media as set out in Surrey Safeguarding Children Board Guidance on using images of children.  
<http://www.surreycc.gov.uk/?a=168635>

### **Use of social media including the school learning platform**

- **The school has a separate social media policy.** (*If a school has its own social media accounts then there should be a separate social media policy covering the use of those accounts.*)
- The school will control access to social networking sites, and consider how to educate pupils in their safe use. This control may not mean blocking every site; it may mean monitoring and educating students in their use.
- Use of video services such as Skype, Google Hangouts and Facetime will be monitored by staff. Pupils must ask permission from a member of staff before making or answering a video call.
- Staff and pupils should ensure that their online activity, both in school and out takes into account the feelings of others and is appropriate for their situation as a member of the school community.

### **Use of personal devices**

- **Personal equipment may be used by staff and/or pupils to access the school IT systems provided their use complies with the online safety policy and the relevant AUP.**
- **Staff must not store images of pupils or pupil personal data on personal devices.**

- **The school cannot be held responsible for the loss or damage of any personal devices used in school or for school business.**

### **Protecting personal data**

- The school has a separate Data Handling Policy. It covers the use of biometrics in school, access to pupil and staff personal data on and off site, remote access to school systems.

### **Policy Decisions**

#### **Authorising access**

- All staff (including teaching assistants, support staff, office staff, midday supervisors, student teachers, work experience trainees, ICT technicians and governors) must read and sign the 'Staff AUP' before accessing the school IT systems.
- The school will maintain a current record of all staff and pupils who are granted access to school IT systems.
- At Key Stage 1, access to the internet will be by adult demonstration with supervised access to specific, approved on-line materials.
- At Key Stage 2, access to the internet will be with teacher permission with increasing levels of autonomy.
- People not employed by the school must read and sign a Guest AUP before being given access to the internet via school equipment.
- Parents will be asked to sign and return a consent form to allow use of technology by their pupil.

#### **Assessing risks**

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor SCC can accept liability for the material accessed, or any consequences of internet access.

#### **Handling online safety complaints**

- Complaints of internet misuse will be dealt according to the school behaviour policy.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of consequences and sanctions for pupils misusing the internet and this will be in line with the schools' behavior policy.

#### **Community use of the internet**

- Members of the community and other organisations using the school internet connection will have signed a guest AUP so it is expected that their use will be in accordance with the school online safety policy.

### **Communication of the Policy**

#### **To pupils**

- Pupils need to agree to comply with the pupil AUP in order to gain access to the school IT systems and to the internet
- Pupils will be reminded about the contents of the AUP as part of their online safety education

**To staff**

- All staff will be shown where to access the online safety policy and its importance explained.
- All staff must sign and agree to comply with the staff AUP in order to gain access to the school IT systems and to the internet
- All staff will receive online safety training on an annual basis

**To parents**

- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.
- Parents' and carers' attention will be drawn to the School online safety Policy in newsletters, the school brochure and on the school web site.
- Parents will be offered online safety training annually.