

# **Greenway Academy On-Line Safety Policy**

**This policy should be read in conjunction with COVID-19 Staff Handbook**

**AND policies below:-**

**Behaviour for Learning  
Anti-Bullying  
Child Protection  
Curriculum  
Data Protection and Security**

**Issued: January 2021  
Approved: December 2020  
Review Date: September 2023**

## **What is On-line safety?**

On-Line Safety encompasses the use of new technologies, internet and electronic communications such as: mobile phones, tablets, collaboration tools and personal publishing. On-Line safety concerns safeguarding children and young people in the digital worlds. It emphasises learning to understand and use new technologies in a positive way, about the risks and the benefits. On-Line safety is concerned with supporting children and young people to develop safer online behaviours both in and out of school.

On-Line Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of on-line safety policy in both administration and curriculum, including secure school network design and use
- Safe and secure broadband including the effective management of filtering.
- The Head Teacher is responsible for the implementation and monitoring of this on-line safety policy.

## **Introduction**

The purpose of this policy is to:

- Through consultation with pupils establish the ground rules we have in Greenway Academy for using the Internet and electronic communications such as mobile phones, tablets, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.
- Describe how these fit into the wider context of our discipline, PSHCE policies and SRE policy.
- Demonstrate the methods used to protect children from sites containing pornography, racist or politically extreme views and violence.
- Understand that accessing inappropriate sites accidentally is not something to feel guilty about and that any such incident should be reported to staff immediately.

## **Teaching and learning**

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school ensures that the use of Internet derived materials by staff and pupils complies with copyright law.

- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Parents are offered lessons on how to help keep their children safe online, with a strong message on encouraging open, honest dialogue between parents and their children now and in the future.

### **Managing Internet Access**

- School ICT systems capacity and security is reviewed regularly.
- Virus protection is updated regularly.

### **E-mail**

- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone.
- E-mail sent to an external organisation must be authorised before sending, in the same way as a letter written on school headed paper.

### **School website**

- CEOP is available on the website and children and parents are taught how, why and when to use.
- The contact details on the Website should be the school address, e-mail and telephone number. Staff or pupils' contact information is not published.
- The head teacher has overall editorial responsibility and ensures that content is accurate and appropriate.
- Photographs that include pupils are selected carefully so they do not enable individual pupils to be clearly identified, unless parental permission has been given.
- Pupils' full names are not used anywhere on the Website or blog.
- Written permission from parents or carers must be obtained before photographs of pupils are published on the school Web site.
- Pupil's work will only be published with the permission of the pupil and parents.

### **Social networking and personal publishing**

- The school blocks access to social networking sites.
- Newsgroups are also blocked.
- Pupils are told never to give out personal details of any kind which may identify them.
- Pupils and parents are advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

### **Managing filtering**

- If staff or pupils discover an unsuitable site, it must be reported immediately to the ICT Subject Leader or a member of the Senior Management Team.
- Senior staff ensures that regular checks are made to ensure that the filtering methods are appropriate and effective.

## **Managing emerging technologies**

- Emerging technologies are examined for educational benefit and a risk assessment is carried out before use in school is allowed.
- Mobile phones are not used during lessons or formal school time by teachers or children. Children are encouraged not to bring their own personal technology into school. When a child takes a phone into school, the child will hand over their mobile phones to the class teacher on entry to the class, where they will be locked away until the end of the school day. In an emergency, a member of staff, from the school office, can release the phone before the end of the day. The school takes no responsibility for the loss or damage of that phone. The sending of abusive or inappropriate text messages is forbidden. Mobile phones are not used during lessons or formal school time by members of staff or pupils.

## **Protecting personal data**

- Personal data is recorded, processed, transferred and made available according to the Data Protection Act 1998.

## **Policy decisions**

### **Authorising Internet access**

- All staff read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- The school keeps a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance if a member of staff leaves or a pupil's access is withdrawn.
- All pupils in the school read and agree to an acceptable use policy when they join the school.
- Access to the Internet will be supervised by a teacher or responsible adult.

### **Assessing risks**

- The school takes all reasonable precautions to ensure that user's access only appropriate material by using CensorNet's filtering system.
- The school audits ICT provision on an annual basis to establish if the on-line safety policy is adequate and that its implementation is effective.

## **Handling on-line safety complaints**

### **Complaints of Internet misuse are dealt with by a senior member of staff.**

- Any complaint about staff misuse is referred to the head teacher.
- Complaints of a child protection nature are dealt with in accordance with the academy's child protection procedures.
- Pupils and parents are informed of the complaints procedure.

## **Communications**

### **Introducing the on-line safety policy to pupils**

- On-line safety rules are posted in all networked rooms and discussed with the pupils at the start of each year.
- Pupils are informed that network and Internet use will be monitored.

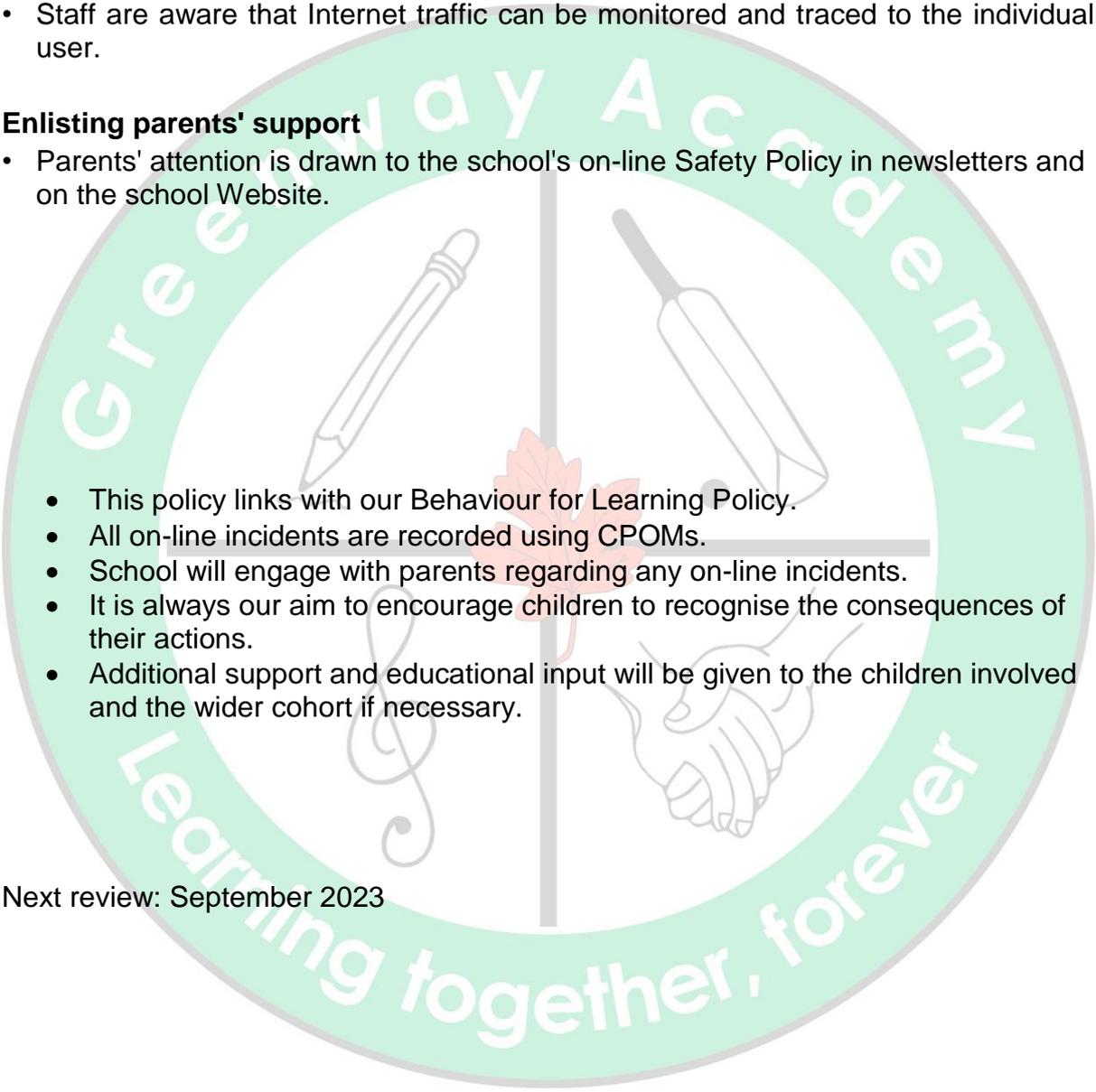
- As part of the National Curriculum and skills development, our pupils and their parents are informed of the child exploitation and online protection centre: [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk)

### **Staff and the on-line safety policy**

- All staff have copies of the school's e-Safety Policy and know its importance.
- The Staff Handbook contains further specific guidance for staff and is considered annually.
- Staff are aware that Internet traffic can be monitored and traced to the individual user.

### **Enlisting parents' support**

- Parents' attention is drawn to the school's on-line Safety Policy in newsletters and on the school Website.

- 
- This policy links with our Behaviour for Learning Policy.
  - All on-line incidents are recorded using CPOMs.
  - School will engage with parents regarding any on-line incidents.
  - It is always our aim to encourage children to recognise the consequences of their actions.
  - Additional support and educational input will be given to the children involved and the wider cohort if necessary.

Next review: September 2023