



# CLEVE HOUSE SCHOOL AND LITTLE CLEVE NURSERY

## E-Safety Policy

### **Introduction**

Computing in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, at Cleve House we need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

E-safety involves pupils, staff and parents making best use of technology, information, training and this policy to create and maintain a safe online and ICT environment for Cleve House and Little Cleve Nursery.

### **Teaching and Learning**

The Internet is an essential element for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils, and so the school has a duty to provide pupils with quality Internet access as part of their learning experience:

The school Internet access will be designed expressly for pupil use including appropriate content filtering.

Pupils will be given clear objectives for Internet use and taught what use is acceptable and what is not.

Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

As part of the new computing curriculum, all year groups have digital literacy units that focus on different elements of staying safe on line. These units include topics from how to use a search engine, digital footprints and cyber bullying.

Through computing we ensure that the school meets the needs of all, taking account of gender, ethnicity, culture, religion, language, sexual orientation, age, ability, disability and social circumstances. It is important that in this school we meet the diverse needs of pupils to ensure inclusion for all and that all pupils are prepared for full participation in a multi-ethnic society.

Pupils are taught in all lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of information

### **Authorised Internet Access**

By explicitly authorising use of the school's Internet access pupils, staff and parents are provided with information relating to e-safety and agree to its use:

Only authorised equipment, software and Internet access can be used within the school. The computers have e-safe education software installed on them which monitors the activity on the computers and sends regular reports to the computing coordinator and Head Teacher. All the computers have the blocksi web filter which provides restrictions for the search content shown and sites allowed.

### **World Wide Web**

The Internet opens up new opportunities and is becoming an essential part of the everyday world for children: learning, homework, sharing are some of the legitimate and beneficial uses. However, there are inappropriate and undesirable elements that must be managed: If staff or pupils discover unsuitable sites, the URL (address), time and content shall be reported to the teacher who will then report to the Headteacher.

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

Pupils will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

### **E-mail**

E-mail is a quick and easy method of communication, ensuring beneficial and appropriate usage is an important part of e-safety:

Pupils may only use approved e-mail accounts on the school system.

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 without specific permission.

Whole class or group e-mail addresses should be used in school rather than individual addresses.

Access in school to external personal e-mail accounts is not allowed.

E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a using outlook.

Chain letters, spam, advertising and all other emails from unknown sources will be deleted without opening or forwarding.

### **Security and passwords**

Passwords should be changed regularly. The system will inform users when the password is to be changed. Pupils and staff should never share passwords and staff must never let pupils use a staff logon. Staff must always 'lock' the PC if they are going to leave it unattended (the picture mute or picture freeze option on a projector will allow an image to remain on the screen and also allow a PC to be 'locked').

### **Social Networking**

Social networking Internet sites (such as, MySpace, Facebook) provide facilities to chat and exchange information online. This online world is very different from the real one with the temptation to say and do things beyond usual face-to-face contact.

Pupils will be advised never to give out personal details of any kind that may identify themselves, other pupils, their school or location. This will also include not using personal photographs and videos.

Pupils will be encouraged to only interact with known friends, family and staff over the Internet and deny access to others.

Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites. The Head teacher will consider taking legal action, where appropriate, to protect pupils and staff against cyber bullying and defamatory comments.

### **Reporting**

All breaches of the e-safety policy need to be recorded in the E-Safety reporting book that is kept in the general office and reported to the designated safeguarding officer. The details of the user, date and incident should be reported.

Incidents which may lead to child protection issues need to be passed on to one of the Designated Teachers immediately – it is their responsibility to decide on appropriate action not the class teachers.

Incidents which are not child protection issues but may require intervention (e.g. cyberbullying) should be reported to the designated safeguarding officer in the same day.

Allegations involving staff should be reported to the Headteacher. If the allegation is one of abuse then it should be handled according to the DFE document titled 'Dealing with allegations of abuse against teachers and other staff'. If necessary the local authority's LADO should be informed.

Evidence of incidents must be preserved and retained.

The curriculum will cover how pupils should report incidents (e.g. Ceop button, trusted adult, Childline)

### **Mobile Phones**

Many new mobile phones have access to the Internet and picture and video messaging. Whilst these are the more advanced features, they present opportunities for unrestricted access to the Internet and sharing of images. There are risks of mobile bullying, or inappropriate contact.

Pupils by permission of the Headteacher can bring mobile phones onto the school site where it is seen by the school and parents as a safety/precautionary use. These are handed into the school office at 8:45 and collected at the end of the day.

The sending of abusive or inappropriate text messages is forbidden.

Staff should always use the school phone to contact parents.

Parents cannot use mobile phones on school trips to take pictures of the children

On trips staff mobiles are used for emergency only

### **Digital/Video Cameras/Photographs**

Pictures, videos and sound are not directly connected to the Internet but images are easily transferred.

Pupils will not use digital cameras or video equipment at school unless specifically authorised by staff.

Publishing of images, video and sound will follow the policy set out in this document under 'Publishing Content'.

Parents and carers are permitted to take photos/videos of their own children in school events. They are requested not to share photos/videos from school events on social networking sites if other pupils appear in the background.

The Headteacher or a nominee will inform parent(s)/guardian(s) and others present at school events that photographs/videos may be taken on the basis that they are for private retention and not for publication in any manner

Staff should always use a school camera to capture images and should not use their personal devices.

Photos taken by the school are subject to the Data Protection act.

### **Published Content and the School Website**

The school website is a valuable source of information for parents and potential parents.

Contact details on the Website will be the school address, e-mail and telephone number.

Staff and pupils' personal information will not be published.

The Headteacher or a nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Photographs and videos that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.

Pupils' full names will not be used in association with photographs.

Consent from parents will be obtained before photographs of pupils are published on the school Website.

Work will only be published with the permission of the pupil.

Parents should only upload pictures of their own child/children onto social networking sites.

The Headteacher may ban the use of photographic equipment by any parent who does not follow the school policy.

### **Information System Security**

School ICT systems capacity and security will be reviewed regularly.

Virus protection will be installed and updated regularly.

### **Protecting Personal Data**

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and Freedom of Information Act

### **Assessing Risk**

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. The school does not accept liability for the material accessed, or any consequences of Internet access.

### **Handling E-Safety Complaints**

Complaints of Internet misuse will be dealt with by a senior member of staff.

Any complaint about staff misuse must be referred to the Headteacher.

Complaints of a child protection nature shall be dealt with in accordance with school child protection procedures.

Pupils and parents will be informed of the complaints procedure.

### **Communication of Policy**

**Pupils:**

Rules for Internet access will be posted in all networked rooms.

Pupils will be informed that Internet use will be monitored.

Pupils will be informed of the importance of being safe on social networking sites. This will be reinforced across all year groups during computing lessons and all year groups look at different areas of safety through the digital literacy lessons.

**Staff:**

All staff will be given the School e-safety Policy and its importance explained.

**Parents:**

Parents' attention will be drawn to the School e-safety on the school Website.

### **Further Resources**

We have found these web sites useful for e-safety advice and information.

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

Set up by the Police with lots of information for parents and staff including a place to report abuse.

**<http://www.childnet-int.org/>**

Non-profit organisation working with others to "help make the Internet a great and safe place for children".

Reviewed: October 2019

Review date: October 2020