CHATHAM & CLARENDON GRAMMAR SCHOOL

# E-SAFETY POLICY

## Reviewed by Governors: November 2023

The aim of our E-Safety policy is to outline the procedures that we have put in place to ensure that pupils and staff can make best use of the ICT facilities available to them in a safe and secure way

The E-Safety Policy is part of the ICT Policy and School Improvement Plan and relates to other policies including those for behaviour, personnel, social and health education (PSHE) and for citizenship. This policy refers to the pupil and staff AUP (Acceptable Use Policy (of the network)) and also the Data Security Policy which should be read in conjunction with this policy.

Our E-Safety Policy has been written by the School, building on the KCC E-Safety Policy and government guidance. It will be reviewed bi-annually.

## 1. Teaching and Learning

**Why is Internet use important?**

- The purpose of Internet use in the School is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the School's management functions.
- Internet use is part of the statutory curriculum and a necessary tool for learning.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- 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.
- Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

**How does Internet use benefit education?**

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;
- educational and cultural exchanges between pupils world-wide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations;

- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with KCC and DfE;
- access to learning wherever and whenever convenient.

**How can Internet use enhance learning?**
We aim to develop effective practice in Internet use for teaching and learning. Librarians and teachers help pupils to learn how to distil the meaning from the mass of information provided by the Internet. Often the quantity of information is overwhelming and staff may guide pupils to appropriate websites. Internet searching skills is part of the Computing curriculum. Above all pupils need to learn to evaluate everything they read and to refine their own publishing and communications with others via the Internet.

- The School Internet access is designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access is planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

## 2. Managing Information Systems

**How will information systems security be maintained?**
The School's Acceptable Use Policy is not currently displayed on all computers as pupils log in but they are expected to adhere to this as part of the overall school policies. Pupils must accept the AUP before access to the computer is granted. In their Computing lessons pupils are taught about good ICT security practice. Sanctions are in place for pupils who break the School's AUP. For staff, flouting electronic use policy is regarded as a matter for dismissal.

From a technical point of view

- Workstations are secured (e.g. C: Drive) and network drives are only available with the correct permissions
- Physical access to servers is restricted.
- The server operating system is secured and kept up to date.
- Virus protection for the whole network is installed, current and continually updated.
- Staff & pupils can access the wireless network with their own devices, however the network is configured to only provide appropriate levels of internet access
- A robust backup system is in place

The School's internet connection is managed in house so that systems are tailored to our needs, including the use of on-premise firewalls, routers and switching equipment.

The security of data is covered in more detail in the Data Security Policy. The following points cover some of the main issues regarding data security

- Personal data sent over the Internet will be encrypted or otherwise secured.
- Data relating to pupils carried on USB Pen drives must be encrypted

- Unapproved system utilities and executable files are not allowed in pupils' work areas or attached to e-mail.
- Files held on the School's network will be regularly checked.
- The ICT co-ordinator / network manager will review system capacity regularly.

**How will e-mail be managed?**
Pupils are taught to use e-mail in year 7 and there are specific references to the use of e-mail in our AUP. 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. Staff must use their School e-mail address for all professional correspondence

- Excessive social e-mail use can interfere with learning and may be restricted.
- E-mail sent to external organisations should be written carefully, in the same way as a letter written on School headed paper.
- The forwarding of chain letters is not permitted.

**How will published content be managed?**
- The contact details on the website will be the School address, e-mail and telephone number. Staff or pupils' personal information are not be published.
- E-mail addresses should be published carefully, to avoid spam harvesting.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website will comply with the School's guidelines for publications including respect for intellectual property rights and copyright.

**Can pupil's images or work be published?**
Images that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. Written permission from parents or carers will be obtained before images of pupils are electronically published. List held by office of pupils who have not given permission for photographs.

**How will social networking and personal publishing be managed?**
The School has blocked access to all social networking sites, access to these sites via proxy servers is specifically outlined in the AUP.

The the exceptions to the ban on social networking are:
1) The use of X (formerly known as Twitter), Facebook and Instagram by the school for self-promotion and news dissemination.
2) The use of X by individual departments to promote the undertakings of said department for the betterment of school image and awareness.

Pupils are advised never to give out personal details of any kind which may identify them and / or their location. This includes real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.

Pupils are advised not to place personal photos on any social network space. They are taught to consider how public the information is and consider using private areas. Advice is given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name or school.

Teachers should not use blogs or wikis as a means of providing content to pupils. This should be done via the School's online platforms.

Pupils are advised on security and encouraged to set passwords, deny access to unknown

individuals and instructed how to block unwanted communications. Students are encouraged to invite known friends only and deny access to others.

**How will filtering be managed?**
Levels of Internet access and supervision will vary according to the pupil's age and experience.

Filtering is handled by on-premise firewalls to ensure that, as much as possible, content is delivered that is appropriate for the pupil. Different levels of filtering are used for each key stage so that pupils are able to search for content relevant to their learning.

Technical staff are able to add blocked sites to our 'allow' list if the member of staff deems that they are suitable. If staff or pupils discover unsuitable sites, the URL must be reported to the E-Safety Coordinator or ICT Manager. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

In addition to Lightspeed another product called 'Securus' is used to maintain a record of pupils accessing or creating inappropriate content, not necessarily web based. Again members of the SLT regularly check logs to ensure that pupils are using the system within our rules

**How can emerging technologies be managed?**
Mobile phones will not be used by pupils during lessons or formal school time, unless part of their lesson. Teachers wanting to use mobile phone technology in their lesson must first discuss the use with their HOD.

The sending of abusive or inappropriate text messages is forbidden.

Staff will be issued with a School phone where contact with pupils is required. Staff must not give their personal mobile number to pupils

**How should personal data be protected?**
For more information on this please see our Data Security Policy.

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

## 3. Policy Decisions

**How will Internet access be authorised?**
The School maintains a current record of all staff and pupils who are granted access to the School's electronic communications. All staff must read and sign the 'Staff Information AUP' before using any School ICT resource.

All pupils must agree to abide by our Acceptable Use Policy each time they login.

Parents of new Yr 7 pupils are asked to sign and return a consent form for pupil access. All pupils who start at any other time will have a consent form in their starter pack

**How will risks be assessed?**
As the quantity and breadth of information available through the Internet continues to grow it is not possible to guard against every undesirable situation. The School addresses the issue that it is difficult to remove completely the risk that pupils might access unsuitable materials via the School system.

The School will take all reasonable precautions to ensure that users access only appropriate

material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a School computer. Neither the School nor KCC can accept liability for the material accessed, or any consequences resulting from Internet use.

The School audits ICT use to establish if our E-Safety policy is adequate and that the implementation of the E-Safety policy is appropriate.

**How will E-Safety complaints be handled?**
Complaints of Internet misuse will be dealt with by a senior member of staff. Any issues of E-Safety regarding pupils will be dealt with in the first instance by the relevant Senior Tutor. Any issues relating to breach of the Acceptable Use Policy will be dealt with by the Deputy Headteacher in charge of E-Learning or the Network Manager. Any complaint about staff misuse will be referred to the Headteacher.

Sanctions regarding cyber-bullying are outlined in the School's anti-bullying policy.

Sanctions for breach of the AUP range between temporary removal of Internet access to temporary exclusion depending on the severity of the offence.

## 4. Communications Policy

**How will the policy be introduced to pupils?**
E-Safety is a crucial part of every pupils' education at the School. Currently the following are used to ensure pupils are aware of the issues:

- Assemblies are held for all year groups on the topic of E-Safety.
- School AUP is displayed each time pupils log in
- The E-Safety policy is available via the School's website
- Links to various E-Safety websites are on the School website
- Parents' information evenings on topic of E-Safety
- Posters around the School highlighting E-Safety
- Pastoral activities and events to promote E-Safety during E-Safety week.

**How will the policy be discussed with staff?**
- All staff will be made aware of the electronic version of the School E-Safety Policy and its application and importance explained.
- Staff are made aware that Internet traffic is be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use are supervised by senior management and have clear procedures for reporting issues. All breaches of E-Safety policy should be reported to a member of the SLT
- Staff training in safe and responsible Internet use and on the School E-Safety Policy will be provided as required.

**How will parents' support be enlisted?**
- Parents' attention will be drawn to the School's E-Safety Policy in newsletters and on the School website.
- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents is encouraged. This includes parent evenings with demonstrations and suggestions for safe home Internet use.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents