Clacton County High School
Walton Road, Clacton-on-Sea, Essex. CO15 6DZ
Tel: 01255 424266 e-mail: admin@cchs.school

Higher Expectations, Raising Aspirations, Transforming Lives

e-Safety Policy

2023-24

This document was last reviewed:	Summer 2023
This document is due for review:	Summer 2024

Clacton County High School is a member of The Sigma Trust
Registered in England and Wales Company No: 7926573
Registered Office: Clacton County High School, Walton Road, Clacton-on-Sea, Essex, CO15 6DZ
e-mail: admin@sigmatrust.org.uk www.sigmatrust.org.uk

Executive Headteacher: Neil Gallagher
Head of School: Chris Taylor

SIGMA TRUST

CONTENTS

e-Safety Policy

Rationale

Information and Communication Technology (ICT) 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. CCHS recognises the need to build in the use of these technologies in order to educate our students with the skills to access life-long learning and employment.

ICT covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast-paced evolution of technology within our society as a whole. Currently the Internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Email, Instant Messaging (e.g. WhatsApp) and chat rooms
- Social Media, including Facebook, Twitter, Instagram, etc
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality
- Gaming, especially online
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading

Whilst exciting and beneficial, both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements (e.g. 13 years for Facebook)
At **CCHS,** we understand the responsibility to educate our students on e-Safety issues, teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the Internet and related technologies.

Writing and Reviewing the e-Safety Policy

The e-Safety Policy relates to the school's safeguarding policies and practices, as well as to other policies including those for ICT, Anti-Bullying and Child Protection.

- A Deputy Headteacher is the school's e-Safety Co-ordinator.
- Our e-Safety Policy has been written by the school, building on government guidance and recommendations. It has been agreed by all staff and approved by Governors.
- The e-Safety Policy and its implementation will be reviewed annually.
- The e-Safety Policy was revised by the Designated Safeguarding Lead (DSL).

Teaching and Learning

Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school will 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 students.
- The purpose of Internet use in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management functions.

Internet use will Enhance Learning

- The school's Internet access will be designed expressly for student use and will include filtering appropriate to the age of students.
- Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Students will be Taught how to Evaluate Internet Content

- The school will ensure that the use of Internet derived materials by staff and students complies with copyright law.
- Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Students 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.

Managing Internet Access

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of students.
- Staff should guide students in on-line activities that will support the learning outcomes planned for the students' age and maturity.
- The school will work with the Internet Service Provider to ensure systems to protect students are reviewed and improved.
- If staff or students discover an unsuitable site, it must be reported to the IT support team or the e-Safety Co-ordinator.
- Senior staff will see that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Communication Technologies School uses a variety of communication technologies and is aware of the benefits and associated risks.

Email:

- Students may only use approved email accounts on the school system.
- Students must immediately tell a teacher if they receive an offensive email.
- Students must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.
- The forwarding of chain emails is not permitted.

Staff Email:

- Only official email addresses are to be used between staff and with students/parents when personal/sensitive data is involved.
- The email has a filtering service that reduces the amount of SPAM (Junk Mail) received on school email accounts. Any incidents of SPAM should be reported to the IT staff.
- All users are aware of the risks of accessing content including SPAM, unsuitable materials and viruses from external email accounts, e.g. Hotmail or Gmail, in school.
- All users are aware that email is covered by The Data Protection Act (2018) and the Freedom of Information Act (2000), meaning that safe practice should be followed in respect of record keeping and security.
- All users are aware that all email communications may be monitored at any time in accordance with the Acceptable Use Policy Appendix 1 within the Sigma Trust Code of Conduct Policy.F
- Our school includes a standard disclaimer at the bottom of all outgoing emails (see below).

****

This email is confidential and may be legally privileged. If you are not the intended recipient, please notify the sender immediately and delete this email and any copies; please note that to disclose, copy or distribute information in this email or to take any action in reliance on its contents is strictly prohibited and may be unlawful. Any views or opinions presented are those of the author only, Clacton County High School cannot guarantee that this email or any attachments are virus free.

Clacton County High School

Clacton County High School is a member of The Sigma Trust.
Registered in England and Wales Company No: 7926573
Registered Office: Clacton County High School, Walton Road, Clacton-on-Sea, Essex, CO15 6DZ
admin@sigmatrust.org.uk www.sigmatrust.org.uk
****

Social Networking and Personal Publishing

Social Network sites allow users to be part of a virtual community. Current popular examples of these are Facebook, Twitter, Instagram and TikTok. These sites provide users with simple tools to create a profile or page, including basic information about the user, photographs, and possibly a blog or comments published by the user. As a user on a social network site, you may have access to view other users' content, send messages and leave comments.

- The school will block/filter access to all social networking sites.
- Students will be advised never to give out personal details of any kind, which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, email address, full names of friends, specific interests and clubs, etc.
- Students and parents will be advised that the use of social network sites outside school have age restrictions for students' own protection (e.g. Facebook – 13 years).

Staff will be made aware of the following:

- They must not give personal contact details to students or parents/carers including details of any blogs, social network accounts or personal websites.
- Adults must not communicate with students using any digital technology, where the content of the communication maybe considered inappropriate or misinterpreted.
- If a member of staff uses a social network site, details must not be shared with students and privacy settings be set at maximum.
- Students must not be added as 'friends' on any social network site.
- Students who request staff as 'friends' should be refused by the staff member and reported to the pastoral hub.

Sending or receiving sexually explicit texts, images or videos via mobile phones, computers or tablets

This is an increasingly common activity among young people, where they share inappropriate or explicit images online or through mobile phones. It is the exchange of self-generated sexually explicit images, through mobile picture messages or webcams over the Internet. Young people may also call it:

- Cybersex
- Sending a nudie, picture or selfie

It is often seen as flirting by children and young people, who feel that it is a part of normal life.

If anyone under the age of 18 years old shares/sends an explicit image of themselves, or an explicit image of anyone else under the age of 18, or engages in any of the behaviours listed above, then the school is duty-bound to consider consulting with the relevant external agencies, i.e. Essex Children's Safeguarding Board, Social Services, the Police. The school's default position will be that it will consult with external agencies should there be a significant age difference between the sender and receiver; if there is any sense of coercion, if the image is of a severe or extreme nature; if the situation is not isolated and the image has been more widely distributed; if it was not the first time an individual had been involved in a sexting act or if there was any malicious intent.

Guidance to parents will be on the website and in newsletters, and students will receive advice and guidance on this in assemblies and form time, PSHE lessons and RSHE lessons.

Mobile Telephone

- The school allows personal mobile phones to be used in school by staff and visitors, but are asked to be left on silent in curriculum time and are not used during lessons.
- It is acceptable to use personal mobile phones for school activities e.g. school trips.
- Personal mobile phones should be locked with a passcode/swipe code.

IT Devices

- Any personal or school owned devices must be locked with a passcode/swipe code.

Online Learning

- There are a variety of applications that staff and students have access to, such as Google classroom, Doddle, Sparx Maths. The IT team have access to all accounts.
- Passwords are issued to the children and they are encouraged not to share their password.
- Students are taught to use applications in a responsible way in conjunction with the e-Safety curriculum.
- Accounts are deleted when staff and students leave the school.

Web Sites and other Online Publications

This may include for example, podcasts, videos and blogs.

- The school website is effective in communicating e-Safety messages to parents/carers.
- Everybody in the school is made aware of the guidance for the use of digital media on the website.
- Staff responsible for editing the website are aware of the guidance regarding personal information and safeguarding.
- Photographs that include students will be selected carefully and will not enable individual students to be clearly identified.
- Students' work and photographs will only be published if the parents/carers have given consent.
- The Executive Headteacher/Head of School have overall responsibility for what appears on the website.

Others

The school will adapt/update the e-Safety policy in light of emerging new technologies and any issues or risks associated with these technologies.

<u>Policy Decisions</u>

Authorising Internet Access

- All staff are bound by the Code of Conduct policy in this regard.
- The school will keep a record of all staff and students who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a student's access be withdrawn.
- Parents and students will be asked to sign and return an 'ICT Acceptable Use Agreement', at the start of Year 7 induction and usually during an admission interview for students who start mid-year.

Assessing Risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT provision to establish if the e-Safety Policy is adequate and that its implementation is effective.

Handling e-Safety Complaints

- Complaints of Internet misuse will be dealt with by a member of the Senior Leadership Team.
- Any complaint about staff misuse must be referred to the Head of School.
- Complaints of a Child Protection nature must be dealt with in accordance with the school's Child Protection procedures.
- Students and parents will be informed of the Complaints Procedure.

Communications Policy

Introducing the e-Safety Policy to Students

- e-Safety rules will be posted in all class rooms and the ICT suite and discussed with the students at the start of each year.
- Students will be informed that network and Internet use will be monitored.
- Termly assembly with an e-Safety theme.

Staff and the e-Safety Policy

- All staff will be given the school e-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to an individual user. Discretion and professional conduct is essential.

Enlisting Parents' Support

- Parents' attention will be drawn to the school e-Safety Policy in newsletters and on the website.
- CCHS website has a large e-Safety section for parents, with information leaflets on sexting, web safety and cyberbullying.