The COUNTY HIGH SCHOOL Leftwich

Achieving Excellence

Document Control Sheet

Document Type	Policy
Document Name	Online Safety
Originator	Laura Kane
Approved by	Full Governing Body
Review interval	Annual
Date of last review	February 2026
Date of next review	Spring 2027
This document is part of the group which include	Safeguarding, Behaviour for Learning, Anti Bullying, Acceptable Use, Exclusions, Policy Statement Additional & Special Education Needs, Drugs' Education, Use of Images, Student Illness, Accident & First Aid, Use of Force, Recruitment, Supporting Children with Medical Conditions, Single Equality Scheme, Searching Screening & Confiscation, Students not attending school due to medical needs, Transgender and Health & Safety Policies. Also part of the group which include Safekeeping of Loaned ICT/AV Equipment and Information Risk Management policies.
Equality Act 2010 fully considered	Yes
EIA Form Completed	Yes

The County High School Leftwich
Granville Road, Northwich, Cheshire, CW9 8EZ
Telephone: 01606 333300

Online Safety

1. **Purpose**

   Online Safety encompasses the use of new technologies, internet and electronic communications such as learning platforms, mobile phones, tablets, video conferencing, collaboration tools and personal publishing. It highlights the need to educate students about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

   1.1. This policy has links to other policies *e.g.* acceptable use, bullying, and safeguarding. There is a Senior Designated Teacher for Child Protection (Mrs M Yates, Assistant Headteacher).

2. **What are the risks?**

Risk	
Content: Student as receiver (of mass productions)	being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism. This also includes content that has been generated for AI.
Contact: Student as participant (adult-initiated activity)	being subjected to harmful online interaction with other users; for example: child on child peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
Conduct: Student as actor (perpetrator / victim)	online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, AI generated harmful content, sharing other explicit images and online bullying,
Commerce:	risks such as online gambling, inappropriate advertising, phishing and or financial scams.
Values The school acknowledges its responsibility to foster informed discussion and protect students from the potential harm caused by extremist* attitudes of all sorts. **The Government has defined extremism in the Prevent Strategy as "…vocal or active opposition to fundamental British Values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs."*	

3. **Requirements on Users**

   3.1. All staff, students and parents/carers must read and sign the acceptable use contract (AUC) before using any of the school's ICT resource.

   3.2. The school has a central record of all staff and students who are granted ICT access. The record will be kept up-to-date, for instance a member of staff may leave or a student's access be withdrawn.

3.3. Students are not permitted under the AUC to use ICT equipment unsupervised.

3.4. Staff and students may only use the school's e-mail accounts on the school's system.

3.5. Mobile Phones are not to be used, heard or seen. If a member of staff sees or hears a mobile phone then the student is required to hand their phone in which will then be returned at the end of the school day. The sending of abusive or inappropriate text messages is forbidden. Use of other personal devices for sound or image recording during formal school time is also prohibited, except under the direction of a teacher.

3.6. Staff will not use non-school personal electronic accounts when contacting students but will use their school email account or, where telephone contact is required, will be issued with a school phone.

4. **Features of the School System**

4.1. Internet access is designed expressly for students and community use and includes filtering both at the remote IT support system and within the school appropriate to the age of the students.

4.2. The school ensures through the AUC that the use of internet derived materials by staff and students complies with copyright law.

4.3. 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. Neither the school nor the remote IT support can accept liability for the material accessed, or any consequences of internet access.

4.4. The school will block/filter access to social networking sites, newsgroups and external email systems. Circumventing this, *e.g.* via proxy servers, is forbidden under the AUC and will result in disciplinary action being taken.

4.5. The school regularly audits ICT provision (in particular remote access logs and website tracking logs).

4.6. School ICT systems are reviewed regularly for capacity and security including virus protection.

4.7. Emerging technologies are examined for educational benefit and a risk assessment highlighting any necessary changes to this policy will be carried out before use in the school is allowed.

5. **Keeping Users Informed**

5.1. Students are taught about what internet use is acceptable and given clear objectives for internet use in both Creative Computing and Media and EfL classes.

5.2. Online safety rules are posted in all rooms where computers may be used and discussed with the students at the start of each year.

5.3. All users are aware via the AUC that internet use is monitored and can be traced to the individual user.

5.4. All staff have access to this Online Safety Policy and its importance will be explained to new staff members.

5.5. Parents'/carers' attention will be drawn to the school's Online Safety Policy when their children join the school and again as appropriate *e.g.* in newsletters, the school web site etc...

6. **Privacy**

6.1. Students must not reveal personal details of themselves or others which may reveal their identity or location in any electronic communication, or arrange to meet anyone without specific permission. They are advised to this effect when signing the AUC as well as in relevant lessons.

6.2. The only contact details on the school web site will be the school address, e-mail and telephone number. Staff or students' personal information will not be published.

6.3. The Headteacher takes overall editorial responsibility for the website and ensures that content is accurate and appropriate.

6.4. Parents' and carers' consent for the publication of photographs of students and their work is obtained on joining the school and photographs of those who opt out are not used.

6.5. Students must not access or copy images used for learning within lessons at any other times.

6.6. Students' full names will not be used anywhere on any school system which is accessible to the public *e.g.* website, particularly in association with photographs.

6.7. The AUC insists that computers be locked when not in use to help prevent unauthorised access to personal data; the lock activates automatically after a set time.

6.8. Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation.

6.9. Staff who choose to access personal data *e.g.* student records from home, or remove such data from site on a removable storage device do so in the knowledge that they are bound by this act and must use an encrypted device.

7. **If something goes wrong...**

7.1. Students must immediately tell a teacher if they receive an inappropriate or offensive electronic communication including e-mail or text messages, including from their peers. **Inappropriate messages will be investigated and when necessary and appropriate, sanctions will be applied (as per Behaviour for Learning policy)**

7.2. If students discover an unsuitable site it must be reported to a teacher and then via the support logging system to the IT Technician who will block/filter the site or escalate as appropriate.

7.3. Complaints of internet misuse will be passed from the class teacher, or IT Technician to the the Designated Safeguarding Lead or Headteacher.

7.4. Complaints about staff misuse will be referred to the Designated Safeguarding Lead, Headteacher or Head's Personal Assistant, as per the Low Level Concerns Policy.

7.5. Complaints of a child protection nature must be dealt with in accordance with the school's safeguarding procedures.

7.6. If any student should approach a member of staff with an allegation involving inappropriate text messages or images of a sexual nature it is not appropriate for that member of staff to attempt to verify the nature of these texts or images by asking to look at them or agreeing to do so if a student or other party offers to show them. The correct response is to pursue the matter promptly with one of our Designated Safeguarding Leads: Mrs Yates; Mrs Kane or Miss Martland. Those members of staff will follow Government Guidance and seek police advice as appropriate.