Online Safety [Appendix F]

The College recognises the importance of safeguarding students from potentially harmful and inappropriate online material and understands that technology is a significant component in many safeguarding and wellbeing issues. The college addresses this by:

- Having robust processes in place to ensure the online safety of students, staff, volunteers
- and governors
- Educating students through the tutorial programme regarding safe and responsible use of
- technology including protecting private information, using social media and how to identify if material is unsafe or biased
- Establishing clear mechanisms to identify, intervene in and escalate any incidents or concerns, where appropriate
- Utilising filtering and monitoring software to respond to concerns. Our approach to online safety is based on addressing the following categories of risk:
  - **C**ontent – being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories
  - **C**ontact – being subjected to harmful online interaction with other users, such as peer-topeer 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
  - **C**onduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
  - **C**ommerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

All staff as part of their induction receive training on online safety which is also embedded into other specific areas such as Prevent and Peer on Peer abuse.

All students, staff, volunteers and visitors sign the acceptable use policy when accessing the college network and systems. Information for parents will be shared on our website regarding our approach to online safety.

Reference QAP 9.1 Online safety

Artificial intelligence (AI) Reference QAP AI 9.3

• Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, students and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini. AI are prohibited from use by staff and students.

• HCFE recognises that AI has many uses, including enhancing teaching and learning, and in helping to protect and safeguard pupils. However, AI may also have the potential to facilitate abuse (e.g. bullying and grooming) and/or expose students to harmful content. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

• HCFE will treat any use of AI to access harmful content or bully students in line with this policy and the college's anti-bullying policy.

• Staff should be aware of the risks of using AI tools while they are still being developed and should carry out risk assessments for any new AI tool being used by the college requirements for filtering and monitoring also apply to the use of AI, in line with Keeping Children Safe in Education.

Safeguarding Incident Procedure for Sexual Imagery

Background

The taking and sharing sexual imagery of children by children is always a risky behaviour and also illegal. Once an image has been shared, control of it has been lost and is unlikely to ever be fully regained. This activity can be more clearly described as 'Youth Produced Sexual Imagery'. NPCC Guidance has been developed to advise forces as to what a proportionate policing response to the investigation of reports of youth produced sexual imagery ('sexting') across England and Wales would look like. It has been designed to enhance the ACPO national position statement published in January 20111. It has been developed in consultation with child protection experts both within and outside law enforcement and also in consultation with children and young people. Separate but interlinked (complimentary) advice for schools has also been developed by CEOP and the UK Council for Child Internet Safety (UKCCIS) education sub group. Police guidance regarding crime recording In January 2016 the Home Office launched a new outcome code (Outcome 21) to help, in part, formalise the discretion available to the police relating to the handling of crimes such as youth produced sexualised imagery.

This policy forms a part of the College's IT strategy and makes it clear that taking, making, sharing and possessing indecent images and pseudo-photographs of people under 18 is illegal. The UK government is working with partner organisations including the Internet Watch Foundation (IWF) and the Marie Collins Foundation to ensure everyone knows the law and understands that:-

• looking at sexual images or videos of under 18s is illegal, even if you thought they looked older

• these are images of real children and young people, and viewing them causes further harm