2023-2024

Hampstead Fine Arts

E-Safety Policy

The aim of this policy is to acknowledge the educational and social benefits of the internet for students but also to balance this with a policy that guides students to the most appropriate use of technology and helps to keep them safe from harm on-line.

This policy should be read in conjunction with the College's policies on *Safeguarding and Child Protection, Staff Safeguarding Code of Conduct, Behaviour and Sanctions, the GCSE and A level Student Contracts, Student and Parent social media Policy, the Behaviour and Sanctions policy.*

Risks of the internet
These can be divided into four categories:

Content
There is material on the Internet that can be harmful to children and young people such as pornography and websites advocating extreme views about violence, religion, racism, self-harm or suicide, and illegal or anti-social behaviour.

Contact
Chat rooms, gaming sites and other social networking sites can pose a risk if young people are 'befriended' by adults whose intention is to groom and/or abuse them. Young people may disclose too much information about themselves or others.

Commerce
Young people may inadvertently give out financial information or passwords or PIN numbers to individuals seeking to carry out fraud or identity theft.

Conduct
Personal online behaviour can increase the likelihood of, or cause harm; for example, making, sending and receiving explicit images, or online bullying (cyberbullying).

Child-on-child abuse
Child-on-child abuse can sometimes be hidden abuse; an online platform is a place where this may happen. Young people need to feel safe online and not fall victim to online abuse of any kind.

College strategy

The aim of the College is to keep all students safe on-line. Safe Internet use is promoted in our programme of PSHCE (Well-being and Enrichment) teaching and in sixth form personal tutorials. We also set out our rules and guidelines about e-safety in the *GCSE and A level Student Contracts,* given to all students and discussed when they join the College. The rules are:

College computers (which are all in a public space, observed by staff at all times) should only be used for activities related to students' studies at the College. They may not be used for social networking or any other non-College-related activities.

The *Staff Safeguarding Code of Conduct* sets out the rules for staff, prohibiting contact between staff and students by personal email, or via social networking sites.

Designated e-safety contact officer

The College's designated e-safety contact officer is Craig Winchcombe (Deputy Head Academic); he liaises closely with the College's Designated Safeguarding Lead, Julie Cope, in this role.

The e-safety contact officer will:

- Monitor and regularly review the College e-safety policy
- Ensure that students and staff are aware that any e-safety incident should be reported to him
- Be the first point of contact for students, staff and parents
- Liaise with the College's IT co-ordinator, Mandy Collinson, about new issues or updates to policy and inform the Principal and Head of these.
- Assess the impact and risk of changing technology and the College's response to these.
- Ensure that all students and staff have read and signed the *e-safety Acceptable Use Policy*
- Maintain a log of internet-related incidents and co-ordinate any investigations into breaches

The College does not have an IT manager. This role is handled by an external IT support company called XMA. Mandy Collinson is in regular contact with the company about IT issues. In accordance with KCSIE 2023 and governmental guidance, Fine Arts has a filtering system (SOPHOS) that restricts access to any potentially harmful content. It also has a firewall installed that is monitored in house and supported by XMA.

Role of College Staff

All staff have a dual role concerning their own Internet use and the provision

of guidance, support and supervision for students. The staff role is to:

- Follow the College's e-safety and Acceptable Use Policy and procedures
- Communicate the College's e-safety and Acceptable Use Policy to students and who to report to
- Keep students safe and ensure they receive the appropriate supervision whilst using the Internet, when necessary
- Use the Internet to plan and research for lessons and, where appropriate, in the delivery of lessons
- Inform the e-safety officer of breaches of Internet use
- Recognise when students are at risk from their Internet use or have had experiences that may cause concern and take appropriate action, such as referral to the e-safety officer
- Teach the e-safety and digital literacy elements of the curriculum in personal tutorials and in PSHCE lessons

Designated Safeguarding Lead and Deputy DSL's

Where any e-safety incident has serious implications for a student's well-being, the matter should be referred to the College DSL, Julie Cope who will liaise closely with the e-safety officer. An investigation will be carried out and the DSL will decide whether a referral should be made to Camden Multi Agency Safeguarding Hub (MASH) and to the Police.

Students with special needs

Students with disabilities and/or learning difficulties may be more vulnerable to risk from use of the Internet and may need additional guidance on e-safety and closer supervision.

The SENDCO will:

- Decide whether any extra requirements for safeguarding or tailored resources and materials are necessary to meet the requirements of any students with special educational needs and/or disabilities.

- Ensure that the College's e-safety policy is adapted to suit the needs of students with special educational needs and/or disabilities.
- Liaise with parents and any other relevant agencies in developing e-safety practices for students with special educational needs and/or disabilities, as required
- Keep up to date with any developments regarding emerging technologies and how these may impact on students with special educational needs and/or disabilities.

Working with parents and guardians

The College will communicate the development and implementation of e-safety strategies and policies to parents and guardians so that they too are aware of Internet risks and are able to continue and reinforce e-safety education at home. The College e-safety policy is made available to parents on the College website, and this is drawn to their attention. This will make parents and guardians aware of the level of their son's or daughter's internet use at College and the expectations regarding their behaviour.

E-safety Policies

Accessing and monitoring the system

- Access to the College Internet is via individual log-ins for staff and via the single student log-in for students. Visitors do not normally have access to the system and permission from either the Principal/Head or the e-safety officer must be sought for this.
- The e-safety officer has access to staff computer log-ins and the student log-in through XMA, our external IT services provider, for the purposes of monitoring and auditing internet activity
- College computers are located in public spaces that are constantly monitored and supervised by staff. Screens are clearly visible to passing staff.
- Students in upper school are only permitted to access the Student wi-fi on their own devices, e.g. tablets and laptops, at tutors' discretion. Lower school students need express permission from the Principal or Head on receipt of an educational psychologist report detailing a specific need to use devices. The *Student Handbook* and student contract on e-safety make clear the expectations of students regarding acceptable internet use. Infringements of the rules will be dealt with as per our *Behaviour and Sanctions* or *Anti-Bullying Policies.*
- Students are not permitted to use the interactive whiteboards or connected laptops in the classrooms without supervision by staff.
- Students are not permitted to use their mobile phones for personal use or as a hotspot in the College buildings. These should be switched off (not on silent mode) and kept out of sight. In the case of Lower School students, Mobiles should be handed in to reception at the beginning of the school day and collected at the end. Students may have their mobile phones during their lunch break.

Acceptable Use Policies

- All students will be expected to sign an Acceptable Use agreement that sets out

their rights and responsibilities and incorporates the College e-safety rules regarding Internet use. (See Appendix 2 and 3 below.)

- All staff will be expected to sign an Acceptable Use agreement that sets out their rights and responsibilities and incorporates the College e-safety rules regarding internet use. (see Appendix 1 below.)
- The e-safety contact officer will ensure all signed Acceptable Use agreements from staff and students will be filed in either individual staff files or student files.

Teaching e-safety

College tutors use all opportunities to discuss and advise students on safe Internet use: in personal tutorials, PSHCE (Well-being and Enrichment) lessons and subject lessons as appropriate.

Personal tutorials and PSHCE lessons include instruction and advice on use of the internet and sites to avoid; social networking including privacy settings and keeping personal information and photographs private, awareness of grooming techniques and instructions on avoiding being drawn into meetings with strangers. They are taught about the problems with cyberbullying and sexting. There is no systems solution to stop the students from using their devices while on the premises and avoiding the student wi-fi to access other sites so teaching safe practice is important.

Information is also given on where to go for help and advice, regarding concerns about the Internet and any communications students may receive or be involved in. See the end of this policy.

Staff Safeguarding Professional Development

The Designated Safeguarding Leader (DSL) Julie Cope and her deputy, Oonagh Ryan, professional development courses on Child Protection every two years that include on-line safety. Training offered by the Local Authority, Camden, is attended annually.

All staff receive 'full' Child Protection and Safeguarding training at least every three years, which includes e-safety. All Staff receive annual updates, or as and when deemed necessary.

Reporting e-safety issues and concerns

Students are advised in the *GCSE and A level Student Contract* to report e-safety issues or concerns to their Head of Year, Personal Tutor or to the College's e-safety Officer. If necessary, they will consult either the DSL or Deputy DSL.

Parents should contact the College's e-safety Officer (Craig Winchcombe) or

the DSL (Julie Cope) or her deputy's (Oonagh Ryan) through the College on 020 7586 0312 or mail@hampsteadfinearts.com

Staff should speak to the College's e-safety Officer (Craig Winchcombe) or the DSL (Julie Cope) or her deputy (Oonagh Ryan) about concerns as soon as possible.

Managing e-safety issues and concerns

This section should be read in conjunction with our *College Safeguarding and Child Protection Policy* and the *Behaviour and Sanctions Policy.*

The e-safety Officer, the DSL and deputy DSL, and if appropriate the student's Head of Year, Personal Tutor, will meet to discuss the concern and the steps that can be taken to advise and protect the student or students concerned.

Members of the Senior Leadership Team (SLT) will become involved if the situation is a particularly serious or difficult one.

Parents of the student or students involved will be notified and consulted and may be called into a meeting with College staff. Searching devices, viewing and deleting imagery will follow the DfE Searching, Screening and Confiscation advice and UKCIS Sexting in Schools and colleges advice.
https://www.gov.uk/government/publications/searching-screening-and-confiscation https://www.gov.uk/government/publications/sexting-in-schools-and-colleges

Cyber-bullying/Child-on-child Abuse

If the on-line issue concerns bullying, the procedures and sanctions outlined in the College *Anti Bullying Policy* and/or *Behaviour and Sanctions Policy* will be used. Please see these policies for more information.

Referral to outside agencies

If an e-safety problem cannot be resolved by College staff and if it is thought that the student or students concerned are at risk of significant physical or emotional harm then the DSL will refer the matter to the Camden MASH team and police.

Referral for early help services will be made in less urgent cases by way of an e-CAF referral to Camden's Early Help/CAF team. Staff will consult with parents prior to making any referral to discuss the matter and gain consent to refer the

child.

Referral for a social work service will be made by way of an e-CAF referral to the CSSW MASH team for children with medium-level needs who are likely to be assessed as being a child in need under section 17 of the Children Act 1989.

Management of personal data

On joining the College, students sign a Data Protection form, allowing the College to use their personal data, if necessary, for on-line applications to the examination boards for access arrangements for exams, such as applications for extra time.

College website

We sometimes use photographs of students on our website. Photographs of students' creative work are also sometimes used on our website or on social media sites such as Flickr. This information is set out in the College's Data Protection Policy available on our website.

Students are not normally identified by name in photographs used on the website and if an individual's name is needed the College would seek express permission for this each time.

Informing and educating parents/guardians about on-line safety

Parents and guardians are asked to read our policies on e-safety, Child Protection, Anti-Bullying and Behaviour and Sanctions, which are made available on the College website and in hard copy from the office.

More information may be obtained by tutors and students from:

The UK Safer Internet Centre (www.saferinternet.org.uk).
https://www.gov.uk/government/publications/teaching-online-safety-in-

schools https://www.gov.uk/government/publications/education-for-a-

connected-world

https://www.gov.uk/government/organisations/uk-council-for-internet-

safety The CEOP's Thinkuknow website **(www.thinkuknow.co.uk).**

April 2024
Reviewed by: JC

Appendix 1

Acceptable Computer Use Policy for College staff

Access and professional use

- All computer networks and systems belong to the College and are made available to staff for educational, professional and administrative purposes only.
- Staff are expected to abide by all College e-safety rules and the terms of this Acceptable Use Policy. Failure to do so may result in disciplinary action being taken against staff.
- The College reserves the right to monitor internet activity and examine and delete files from the College's system.
- Staff have a responsibility to safeguard pupils in their use of the internet and report all e-safety concerns to the Designated Safeguarding Lead.
- Copyright and intellectual property rights in relation to materials used from the internet must be respected.
- E-mails and other written communications must be carefully and professionally written and polite in tone and nature.
- Anonymous messages and the forwarding of chain letters are not permitted. • Staff will have access to the internet as agreed by the College but will take care not to allow pupils to use their log-in to search the internet.
- Staff should not use mobile phones inside the College buildings

Data protection and system security

- Staff should ensure that any personal data sent over the internet will be encrypted or sent via secure systems. Where personal data is taken off the school premises via laptops and other mobile systems, the information must be encrypted beforehand.
- Use of any portable media such as USB sticks, External Hard Drives, et al is permitted where virus checks can be implemented on the College ICT system using SOPHOS software.
- Downloading executable files or unapproved system utilities will not be allowed and all files held on the College system will be regularly checked. • Sharing and use of other people's log-ins and passwords is forbidden without permission, Users should ensure that they log-out when they have finished using a computer terminal.
- Files should be saved, stored and deleted in line with College policy.

Name:

Signed:

Date:

Appendix 2

Acceptable Computer Use Policy for Fine Arts College students

I understand that all computer equipment is owned by the College and that I can use the internet at College as long as I behave in a responsible way that keeps me and others safe. I also understand that the College ICT system is monitored and that if I do not follow the rules there may be consequences in the form of sanctions.

I will:

- use the College's computers only for College work and homework • only access/delete my own files and not look at other people's files without their permission
- always switch to the student log-in for College computers
- not bring in data files to College without permission
- ask a member of staff for permission before using the internet on College computers
- only visit websites that are approved by a tutor
- make sure any messages I send by any electronic means are not hurtful or abusive
- be aware that anything posted on-line is public and permanent
- tell a tutor or the DSL if I see anything I am unhappy with or receive a message I do not like; I will not respond to any bullying messages
- keep my mobile switched off and out of sight in College
- not make any derogatory or disparaging comments on social media or any other public forum about the College, its staff or pupils, or in any other way breach the

College's social media Policy log out when I have finished using a College computer.

Name:

Signed:

Year group:

Date:

Appendix 3

Acceptable Computer Use Policy for Fine Arts Lower School students

I understand that all computer equipment is owned by the College and that I can use the internet at College as long as I behave in a responsible way that keeps me and others safe. I also understand that the College ICT system is monitored and that if I do not follow the rules there may be consequences in the form of sanctions.

I will:

- use the College's computers only for College work and homework • only access/delete my own files and not look at other people's files without their permission
- always switch to the student log-in for College computers
- not bring in data files to College without permission
- ask a member of staff for permission before using the internet on College computers
- only visit websites that are approved by a tutor
- make sure any messages I send by any electronic means are not hurtful or abusive
- be aware that anything posted on-line is public and permanent
- tell a tutor or the DSL if I see anything I am unhappy with or receive a message I do not like; I will not respond to any bullying messages
- hand in my mobile at registration in the morning and get it back at the end of the school day
- not make any derogatory or disparaging comments on social media or any other public forum about the College, its staff or pupils, or in any other way breach the

College's social media Policy log out when I have finished using a College computer

- get permission from the Principal/Head if I need to use my own laptop in class and can provide an educational psychologist's report detailing the need.

Name:

Signed:

Year group:

Date: