E-SAFETY POLICY

Document Control	
Manager responsible	Tina Tupper, ILT Manager
Version number	2.0
Approved by	SLT
Approval date	07 October 2020
Review date	October 2021

E-Safety Policy

Contents Page

1 Introduction:

Hereford College of Arts recognises the benefits and opportunities which new technologies offer to teaching and learning and assessment. We encourage the use of technology in order to enhance skills and promote achievement. However, the accessible and global nature of the internet and variety of t evolving technologies and media available mean that we are also aware of potential risks and challenges associated with such use. Our approach is to implement safeguards within the college and to support staff and students to identify and manage risks independently. We believe this can be achieved through a combination of security measures, training and guidance and implementation of our associated policies. In furtherance of our duty to safeguard students which includes the latest 'Keeping Children Safe in Education' and Prevent Duty guidance, we will do all that we can to make our students and staff stay e-safe and to satisfy our wider duty of care. This e-safety policy should be read in conjunction with other relevant college policies e.g. Safeguarding and Child Protection, Prevent, IT Acceptable Use, IT Security and Student Disciplinary Code.

2 Creation, Monitoring and Review

The college e -Safety Policy has been written following consultation with the Designated Safeguarding Lead and Deputy, the Senior Management Team, the HE Management Team, the FE Management Team and the Well Being Development Lead.

Approval procedure:

SLT

Academic Board

Board of Governors

The impact of the policy will be monitored regularly with a full review being carried out once a year. (The policy will also be reconsidered where an e-safety incident has been recorded or there has been a change in the legal framework).

3 Policy Scope

The policy applies to all students, staff and all members of the college community who have access to the college IT systems, both on the premises and remotely. Any user of college IT systems must adhere to the e-Safety Policy, IT Security Policy and the Acceptable Use Policy provided. The e-Safety Policy applies to all use of the internet and electronic communication devices such as email, mobile phones, games consoles and social networking sites.

4 Roles and Responsibilities

There are clear lines of responsibility for e-safety within the college, direct responsibility lies with the ILT Manager. However, all staff have a shared responsibility for ensuring the safety of students and should report any concerns immediately to their line manager and report the concern through 'MyConcern' to the DSL team. All teaching staff are required to deliver e-safety guidelines to students as part of the curriculum. When informed about an e-safety incident, staff members must take particular care not to guarantee any measure of confidentiality towards either the individual reporting it, or to those involved.

All students must know what to do if they have e-safety concerns and who to talk to. In most cases, this will be their course tutor. Where any report of an e-safety incident is made, all parties should be made aware of procedures and how these will be acted upon. Where management considers it appropriate, the SLT Lead for Safeguarding may be asked to intervene with appropriate additional support from external agencies.

SLT Lead for Safeguarding:

The ILT Manager in conjunction with the SLT Lead for Safeguarding is responsible for promoting and monitoring e-Safety, delivering staff development and training, recording incidents, reporting any developments and incidents and liaising with the local authority and external agencies to promote e-safety within the college community.

Students:

Students are responsible for using the college IT systems and mobile devices in accordance with the college Acceptable Use Policy, IT Security Policy and the e-Safety policy, (available on the college website and VLE) which they must agree to. They are expected to seek support and follow procedures where they are worried or concerned, or where they believe an e-safety incident has taken place involving them or another member of the college community. Students must act safely and responsibly at all times when using the internet and/or mobile technologies.

Staff:

All staff are responsible for using the college IT systems and mobile devices in accordance with the college Acceptable Use, IT Security and E-safety policies, which they must actively promote through embedded good practice. Staff are responsible for attending staff training on e-safety and displaying a model example to students at all times.

All digital communications with students must be carried out in line with the college policies and procedures and be professional in tone and content at all times with due regard to issues of safeguarding and defamation. Online communication with students is restricted and must only be done through the college resources and the VLE. Staff are not permitted to create their own course pages for Social Networking without informing

the Communications Team who will advise on how to set up the page responsibly. Staff should not invite students as friends to their personal Social Networking pages. Staff may accept invite requests from Students to their professional pages only. The college will provide Social Networking pages for certain resources which will be monitored by the Communications team. Staff should exercise great caution in using online or social media to communicate with students and in particular they should in no circumstance use personal mobile phone numbers, social media or email contacts to communicate with students under the age of 18 years.

5. Security

The college will do all that it can to make sure the college network is safe and secure. Every effort will be made to keep security software up to date. Appropriate security measures will include the use of enhanced filtering and protection of firewalls, servers, routers, work stations etc. to prevent accidental or malicious access of college systems and information. Digital communications, including email and internet postings, over the college network, will be monitored in line with the IT security policy available on the college VLE.

Web filtering software is installed to ensure students are able to access online information in a safe and secure environment. The Network Manager and ILT Manager receive regular reports outlining any attempts to access information blocked by the filters. Web filtering categories are detailed in the Appendix. Immediate action will be taken if any activity seeking to promote hate crimes, terrorism and radicalisation which includes extremist websites and searching/viewing of inappropriate material, exploitation, fraud or offence has been recorded and will be reported to SLT. When delivering teaching and learning remotely, staff should remain aware of the Safeguarding, Child protection and Prevent Policy.

7 Behaviour

Hereford College of Arts will expect that all users of technologies adhere to the standard of behaviour as set out in the IT Acceptable Use Policy or Student Disciplinary Code on the college VLE.

Measures have been taken to prevent staff or students from obtaining material that could lead to sexual exploitation, radicalisation or terrorism through our web filtering software. Should anyone obtain access to such material the college has ensured that staff and students have had the appropriate training to report such incidences as set out in the Safeguarding, Child protection and Prevent Policy.

The college will not tolerate any abuse of IT systems. Whether offline or online, communications by staff and students should be courteous and respectful at all times. Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and in line with the student and staff disciplinary codes.

Where conduct is found to be unacceptable, the college will deal with the matter internally. Where conduct is considered illegal, the college will report the matter to the police.

8 Communications

All forms of communication, including email and text messaging, should always be used in a professional manner and not reflect negatively on the college.

The use of mobile phones is permitted within college but staff and students should always ensure that they are professional and courteous when using them and be aware of the implications of their misuse. Recording of images, sound or film using mobile devices should only be done with the consent of those present.

The college will consider any personal information made available on Networking sites or Blogs to be in the Public Domain. Members of the college community (staff/students) should ensure that any such information does not bring the college or its reputation into disrepute. Any defamatory information transmitted by members of the college community could face disciplinary or legal action.

9 Use of Digitally recorded material (including sound, pictures, moving image and live streaming)

The use of images, or photographs, is popular in teaching and learning and should be encouraged where there is no breach of copyright or other rights of another person. This will include images downloaded from the internet and images belonging to staff or students.

All students and staff should receive training during the induction process on the risks in downloading these images as well as posting them online and sharing them with others. For example, there are particular risks where personal images are posted onto social networking sites.

The Hereford College of Arts staff will provide information to students on the appropriate use of images as detailed in the Learner Agreement. Our aim is to reinforce good practice as well as offer further information for all users on how to keep their personal information safe.

Digital recordings of anyone at college must not be taken without their knowledge or consent, unless there is a risk of criminal activity (CCTV). The use of such recordings for any purpose which may cause offence, embarrassment, distress or harm to another student, tutor, parent or visitor, may put the user at risk of prosecution under current legislation. Any student publishing or circulating recorded material which cause offence, embarrassment, distress or harm to another student, teacher, parent or visitor may face disciplinary action.

Staff and students will have the ability to request that their personal digital material should not be used for by the college for Social Media or other promotional purposes.

The college adheres to General Data Protection Regulations (GDPR) and takes great care to ensure privacy is respected.

10 Personal Information

Personal information is collected and stored by Hereford College of Arts for administrative purposes only, including for example names, dates of birth, email addresses, personnel files, assessment materials and so on. The college will keep that information safe and secure and will not pass it onto anyone else without the permission of the individual concerned.

No personal information can be posted to the college website without the permission of that individual. Only names and work email addresses of essential staff or services will appear on the college website.

Staff must keep students' personal information safe and secure at all times. When using an online platform, all personal information must be password protected. Every user of IT facilities is required to log off on completion of any activity, or where they are physically absent from a device.

Any mobile device (laptop, USB) should be password protected and signed out by the IT or Media Store staff.

Where the personal data is no longer required, it must be securely deleted in line with the Data Protection policy.

11 Education and Training

With the current unlimited nature of internet access, it is not possible for the college to eliminate all risks for staff and students, however the college recognises its duty to safeguard its community through the management and understanding of those risks. It is our view therefore, that the college should support staff and students through training, education and effective IT systems. This will provide them with the tools and skills to be able to identify risks independently and manage them effectively.

For students:

All students will receive a H&S Induction during the induction period and before accessing the college systems and includes issues associated with e-safety, with guidance on what precautions and safeguards are appropriate when making use of the internet and technologies. Students should also know what to do and who to talk to where they have concerns about inappropriate content, either where that material is directed to them, or where it is discovered as part of a random search. The college e-Safety Policy is available on the college website and VLE with key information highlighted in posters and leaflets around open plan IT areas and work stations.

Within sessions, students will be encouraged to question the validity and reliability of materials researched, viewed or downloaded. They will also be encouraged to respect the copyright of other parties and to cite references properly.

For staff:

E-safety advice is given to all new staff as part of their induction process. Further resources of useful guidance and information is available on the college VLE. Any new or temporary users will receive training on the college IT system and e-safety. They will also be asked to sign that they have received and read the college Acceptable Use, IT Security and e-Safety policies.

12 Incidents and Response

Where an e-safety incident is reported the college will act immediately to prevent any harm from occurring. If a learner wishes to report an incident, they can do so to their course tutor, a member of the Safeguarding & Prevent Committee or to the college SLT Lead for Safeguarding. Where a member of staff wishes to report an incident, they must contact their line manager. Following any incident, the college will review what has happened and decide on the most appropriate and proportionate course of action. The matter will be investigated and if necessary, sanctions put in place. This is in line with the college Acceptable Use Policy, Safeguarding and prevent Policy and Student Disciplinary Code. Senior management, in consultation with appropriate external agencies, will deal with serious incidents.

13 Further Information

Useful Links for Further Information:

Child Exploitation & Online Protection Centre

Internet Watch Foundation

Get Safe Online

Keeping Children Safe in Education

14 Appendix: Sophos Blocked Categories

- Anonymizers
- Extreme
- Hacking
- Intellectual Piracy
- Intolerance & Hate
- Legal highs
- Marijuana
- Militancy & Extremist
- Nudity
- Parked Domain
- Phishing & Fraud
- Pro-Suicide & Self-Harm
- Sexually Explicit
- Spam URLs
- Spyware & Malware
- Swimwear & Lingerie
- Unauthorised Software Stores
- Weapons
- Pro-Anna (Sites that promote Anorexia)