Hereford
SIXTH FORM COLLEGE

ONLINE SAFETY (LEARNER) POLICY AND PROCEDURES

2022/23

Responsibility

SMT member: **Director of Safeguarding, Inclusion and Development**
Working with: **All staff and students**

Aim

One of the main applications of technology that young people use today is the internet. Hereford Sixth Form College acknowledges that staying safe online is an increasingly complex issue and are committed to educating and supporting students in online matters.

Scope

This policy applies to all students within the College community who have access to the College IT systems, both on the premises and remotely and applies to all use of the internet and forms of electronic communication such as email, mobile phones, social media sites and mobile devices.
All users of College IT systems are required to agree to adhere to these policy and regulations and have to hand within their student handbook a clear guide to Internet safety and the risks associated with its use.

Policy Statement

Hereford Sixth Form College recognises the benefits and opportunities which new technologies offer to teaching and learning. We provide internet access to all students and staff and encourage the use of technologies in order to enhance skills, promote achievement and enable lifelong learning. Our approach is to implement appropriate safeguards within the College while supporting students to identify and manage risks independently and with confidence.

Students will have access to the Internet and email on all networked computers and mobile device technology used in the College for research and education purposes and HSFC welcomes this as a means of improving the IT skills of users and as an aid to teaching and learning. Students may also access the College wireless network on their mobile devices in order to access the internet.

Students will receive an induction to IT Services provided at the College during one of their initial Group tutorial sessions. They are given a user name for the Computer Network and must agree to abide by the *Acceptable Use Policy* (Student & WiFi) and this policy as part of their induction process.

All students will be educated on online safety through online lessons which they all undertake as part of their Tutorial programme.

Roles and Responsibilities

There are clear lines of responsibility for online safety within the College.

All students must know what to do if they have online safety concerns and who to talk to (see Appendix 1 for details of key personnel who have specific e-safety responsibilities at HSFC). In most cases, incidences and concerns which are raised by students with regards to their online safety (e.g. bullying/harassment, grooming) will be dealt with by the allocated Lead Tutor or in their absence the designated person with responsibility for safeguarding. Where any report of an online safety incident is made, all parties should know what procedure is triggered and how this will be followed up. This will be discussed with the student/person reporting the incident.

Where management considers it appropriate, the designated persons may be asked to intervene with appropriate additional support from external agencies including the Police.

- Students are responsible for using the College IT systems and mobile devices in accordance with the *Acceptable Use Policy* (Student & WiFi) which they must sign at the time of registration.
- Students must act safely and responsibly at all times when using the internet and/or mobile technologies.
- Students are responsible for attending online safety lessons as part of their Tutorial programme and are expected to know and act in line with other relevant College policies with regards to online safety matters and in particular mobile phone use, sharing images, cyber-bullying etc.
- Students must follow reporting procedures where they are worried or concerned, or where they believe an online safety incident has taken place involving them or another member of the College community. Further guidance is available in the flow chart in Appendix 1.

IT systems monitoring and filtering

As stated in the Acceptable Use Policy (Student & WiFi) the College has a statutory duty to carry out appropriate filtering and monitoring to keep students safe and free from harm. The college recognises its responsibilities set out in Keeping Children Safe in Education (2021) which requires us to identify potential risk in the ICT environment, intervening and escalating any concerns raised as necessary. The guidance recognises identifies four categories of online risk that school staff and students should be aware of:

- **CONTENT**: being exposed to illegal, inappropriate or harmful material
- **CONTACT:** being subjected to harmful online interaction with other users

- **CONDUCT:** personal online behaviour that increases the likelihood of, or causes, harm.
- **COMMERCE:** being exposed to inappropriate advertisement, online gambling & financial scams

The College therefore has effective monitoring software which is operational on college devices so that we can fulfill these requirements and support and intervene when any safeguarding reports are initiated through the software. The software monitors use of College devices and identifies any safeguarding concerns and issues (cyberbullying, radicalisation, abuse) which may result in reports being made and send to the Designated Safeguarding Lead and Deputy Safeguarding Leads for consideration so that any incidences can be acted upon swiftly and escalated and reported as appropriate. Reports of any safeguarding, child protection concerns are produced in real time so that any concerns identified can be dealt with immediately with students/users. The designated Governor, in collaboration with Hereford Sixth Form College's Chair of Governors, is responsible for ensuring the College has appropriate IT filters and monitoring systems in place.

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.

Students should use strong passwords for any IT accounts including their college password. These are long (at least 8 characters) and have a combination of upper and lower case letters, numbers and one or more special keyboard characters such as the asterisk or currency symbols.

All College mobile devices such as a laptop, USB (containing personal data) are required to be encrypted, password protected and signed out by a member of the IT staff before leaving the premises.

Behaviour

Hereford Sixth Form College will ensure that all users of technologies adhere to the standard of behaviour as set out in the *Acceptable Use Policy* (Student and WiFi) and this 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 *Anti-Bullying and Harassment Policy and Procedures* and *Acceptable Use Policy* (Student and WiFi)

Where conduct is found to be unacceptable, the College will deal with the matter internally. Where conduct is considered illegal, the College will seek advice, support and guidance appropriately, report the matter to the police and any other relevant external agencies.

Social Media

Social Media sites are powerful tools that, if used in the correct 'safe' way, can be a great way to socialise, broadcast, share, voice opinions, and network. However, they can also be very dangerous if used incorrectly ruining relationships and potentially affecting future career and university options.

The College have a number of Social Media sites which are used to support teaching and learning in a number of curriculum areas. Each site has a lead person who is responsible for its content and all users (student and staff) of these sites must abide by the Social Media guidelines set out below.

The following is a set of guidelines to help students safely enjoy social media:

Do

- Regularly check and change your privacy settings.
- Be respectful to others online, to others and yourself.
- Use a strong password and change it regularly.
- Read the privacy policy of the site.
- Check the privacy policy and authenticity of apps that you may add.
- Remember what you post can affect you in the real world, universities and future employers may check your social media profiles.
- ALWAYS report cyber bullying to an adult/teacher/parent/guardian/DoS.

Don't

- Let your friends pressure you into doing something on social media sites that you are not comfortable with.
- Leave your profile logged in, if you are using your smart phone to access social media, password protect your phone.
- Never click on links or install applications that are sent to you if you're not expecting them.

Use of Images and Video

The use of images, or photographs, is popular in learning and should be encouraged where there is no breach of copyright or other rights of another person (e.g. images rights or rights associated with personal data). This will include images downloaded from the internet and those belonging to staff or students.

All students will receive training in their online safety session incorporated into the Tutorial programme which considers the risks when taking, downloading and posting images online and making them available to others. There are particular risks where personal images of themselves or others are posted onto social networking sites, for example.
The College requires all students to check and comply with copyright laws when using any images within their classwork, homework, coursework or other College activity. This includes images downloaded from the internet and images belonging to staff or students.

Education and Training

With the current unlimited nature of internet access, it is impossible for the College to eliminate all risks for students. It is our view therefore, that the College should support students to stay safe through regular training and education. This will provide students with skills to be able to identify risks independently and manage them effectively.

Students will attend online safety sessions within the Tutorial programme which is compulsory for all students within College. The first of these will take place during the first half term at the beginning of the College year.

Issues associated with online safety apply across the curriculum and students should receive guidance on what precautions and safeguards are appropriate when making use of the internet and technologies within their academic areas.

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. A link to the College online safety policy will be accessible on the VLE for all students use and key safety messages are highlighted in posters and leaflets around College.

Within classes, 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.

Online safety advice to parents has also been compiled and is contained on the College website and parents are signposted to this information through the Parents Handbook which is distributed to them following enrolment.

Incidents and Response

Where an online safety incident is reported to the College this matter will be dealt with very seriously.

The College will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring. If a student wishes to report an incident, they can do so to their Lead Tutor or the Network Manager/Network Administrator according to the Incident report flow chart in Appendix 2.

Following any incident, the College will review what has happened and decide on the most appropriate and proportionate course of action. Sanctions may be put in place, external agencies may be involved or the matter may be resolved internally depending on the seriousness of the incident. Serious incidents will be dealt with by senior management, in consultation with appropriate external agencies.

Related Policies and Procedures

This online safety policy should be read alongside other relevant College policies:

- *Safeguarding and child protection Policy and Procedures*
- *Anti-Bullying and Harassment Policy and Procedures*
- *Acceptable Use Policy (Student and WiFi) and Procedures*
- *Data Protection Policy and Procedures*
- *Peer on Peer abuse Policy*

Appendix 1

Key roles and responsibilities for eSafety at Hereford Sixth Form College

Helen Osborn	Designated Senior Lead for Safeguarding hmm@hereford.ac.uk
John Pratt	Deputy Designated Safeguarding Lead jpp@hereford.ac.uk
Phil Tranter	Deputy Designated Safeguarding Lead pjt@hereford.ac.uk
Ruth Figg	EMedia Coordinator and HMT DPO rb@hereford.ac.uk
Mark Ridgway	Director of IT & MIS mjr@hereford.ac.uk
Duncan Childs	MIS Manager & Data Protection Representative for HSFC dc@hereford.ac.uk
Dunstan Lawrence	Network Manager dbl@hereford.ac.uk

Appendix 2

Online safety incident/ concern identified through monitoring and filtering software or raised by Student or Member of staff

Students Personal Tutors to be informed, in the case member of staff their line manager to be informed. Personal Tutor to inform DoS/Line manager to liaise with online coordinator and Network Manager/Network administrator as appropriate to carry out investigation and for any action to be taken

Inappropriate material suspected or behavioural concerns including harassment, Cyber bullying, inappropriate comments (racist, homophobic, discriminatory in any way or defamation).

Deemed to be Illegal materials/activities (including grooming, sexually explicit material shared with child, child abuse images)

DoS/ Line Manager to review incident and discuss and agree appropriate action plan and course of action, apply sanctions according to College Anti-Bullying and Harassment Policy if appropriate and College disciplinary procedures including exclusion policy and procedures. In more serious cases reports may be made to the Police

Illegal activity

Illegal Content

Student at Risk

Report incident to Police for investigation

Report to Internet Watch Foundation (IWF.org,uk), and inform local Police. Social media reporting mechanisms used if appropriate .

Referral to be made directly CEOP, Police and Local Safeguarding Childrens/ Adult board as appropriate.

Record of incident to be kept and advice to be followed from external agency regarding securing and preserving evidence until it can be reviewed and investigated

Possible internal action depending on nature of incident:

- Inform parents/carers
- Review incident to attempt to prevent further incidences
- Referral for counselling or other support services and external agencies as appropriate
- In case of report made by member of staff or against a member of staff, student or staff disciplinary action to be followed depending on nature of incident reported
- Record of incident to be kept for reference and monitoring
- Any appropriate action will be taken in liaison with and collaboration with external agencies depending on nature of incident reported especially when dealing with illegal activity, content and if the student is deemed to be at risk of harm.

Review of incident and online concern raised, records kept for future monitoring

Review Policies and procedures, technical tools and monitoring methods and make changes if appropriate.