WORCESTER
SIXTH FORM COLLEGE

e-Safety Policy

E-SAFETY POLICY

1. Introduction

Worcester 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. However, the accessibility and global nature of the internet and different technologies available mean that we are also aware of potential risks and challenges associated with such use. Our approach is to implement appropriate safeguards within the college while supporting staff and students to identify and manage risks independently and with confidence. We believe this can be achieved through a combination of security measures, education and training, guidance and implementation of our policies. In furtherance of our duty to safeguard students and the Prevent duty, we will do all that we can to enable our students and staff to stay e-safe and to satisfy our wider duty of care.

This e-safety policy should be read alongside other relevant college policies including the following:
Acceptable Use Policy for Staff – available in Repository/College Policies/Employment
Acceptable Use Policy for Students and Visitors – available on the e-Safety section of the College Website, and in Repository/College Policies/Student Support
Anti Cyber-Bullying Code - Appendix A
Code of Conduct for Students – Repository/College Policies/Student Support & Guidance
Code of Conduct for Staff – Repository/College Policies/Employment
Data Protection Policy – Repository/College Policies/Management
Safeguarding Policy – Repository/College Policies/Management

2. Creation, Monitoring and Review

The impact of the policy will be monitored regularly with a full review being carried out at least once a year. The policy will also be reconsidered where particular concerns are raised or where an e-safety incident has been recorded.

3. Policy Scope

The policy applies to all students and staff who have access to the college IT systems, both on the premises and remotely. Any user of college IT systems must agree to and adhere to the Acceptable Use Policy for Students and Visitors and/or the Acceptable Use Policy for Staff, in addition to this e-Safety Policy. The e-Safety Policy applies to all use of the internet and forms of electronic communication such as email, mobile phones, and social media sites.

4. Roles and Responsibilities

There are clear lines of responsibility for e-safety within the college. The first point of contact should be the e-Safety Officer & Designated Safeguarding Lead.

e-Safety Officer:

The e-Safety Officer (who is also the Designated Safeguarding Lead) is responsible for keeping up to date with new technologies and their use, as well as attending relevant training. They lead the e-Safety Group, complete, review and update the e-Safety Policy and Action Plan, deliver staff development and training, record incidents, report any developments and incidents to the Principal and liaise with the local authority and external agencies to promote e-safety within the college community. The e-Safety Officer is also responsible for determining the College's response to any e-Safety incident.
e-Safety Group:

- **e-Safety Group**

The e-Safety Group, under the lead of the e-Safety Officer,exists to promote the College's policies and procedures in relation to e-Safety. The group is a forum for discussion and has no executive or governance function. It consists different stakeholders including the e-Safety Officer & Designated Safeguarding Lead, the Deputy Principal, the IT Support Manager, the ILT Co-ordinator, and several student representatives. Thee-Safety Group considers policies relating to e-Safety, proposing amendments and updates as required, it regularly updates the action plan and follows up where further action is required, and it consults staff and student views on aspects of e-Safety. It meets every term, or more often as required.

Students:

Students are responsible for using the college IT systems and mobile devices in accordance with the Acceptable Use Policy for Students and Visitors, which they must agree to at the time of course confirmation (or after any significant change to the Policy) and this e-Safety Policy. Students must act safely and responsibly at all times when using the internet and/or mobile technologies.

Students are responsible for attending e-safety lessons as part of the tutorial programme and curriculum and understanding and following the e-safety guidelines issued by the College. Students are expected to know and act in line with other relevant college policies e.g. Anti Cyber-bullying Guide **(see Appendix A)**.

If students have e-safety concerns regarding themselves or another member of the College community they must talk to their teacher, tutor, Head of Year, e-Safety Officer & Designated Safeguarding Lead, or other member of SMT. If the report of an e-safety incident is made in relation to cyber-bullying the relevant Head of Year will determine the appropriate response, seeking guidance from the e-Safety Officer and Designated Safeguarding Lead as appropriate. Where the report is of a general e-Safety incident then staff indicates any risk to or repercussions for student well-being then the incident must be referred to the e-Safety Officer and Designated Safeguarding Lead who will determine the appropriate response directly. Where management considers it appropriate, the e-Safety Officer & Designated Safeguarding Lead may be asked to intervene with appropriate additional support from external agencies.

Staff:

All staff are responsible for using college IT systems and mobile devices in accordance with the Acceptable Use Policy for Staff, which they must agree to at the beginning of the College year (or after any significant change to the Policy or any subsequent commencement of employment at College) and this e-Safety Policy.

Staff are responsible for attending staff training on e-safety and displaying a model example to learners at all times through embedded good practice. All teaching staff are required to deliver an e-safety lesson to their classes and to ensure that they have at least 1 research activity that informs students of the principles of e-safety.

All staff are responsible for ensuring the e-Safety of students and should report any concerns immediately to the e-Safety Officer & Designated Safeguarding Lead (or if this is not possible they should report concerns or incidents to their line manager or a member of the Senior Management Team). 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.

Staff must take responsibility for, and be committed to, promoting and safeguarding the welfare of children, young persons and vulnerable adults whether responsible for, or in contact with, them. Staff must not ignore, initiate or encourage extremism. This includes the requirement to be alert to the risks of how students can be drawn into extremism and to pass any suspicions or relevant information to the Single Point of Contact, the Designated Safeguarding Lead & e-Safety Officer, or, in her absence, any member of the College's Safeguarding Team or Senior Management Team.

All digital communications with learners must be professional at all times and be carried out in line with the Acceptable Use Policy for Staff. External platforms not hosted by the college, such as social media

sites, must only be used for communication with students in accordance with the Acceptable Use Policy for Staff. In particular staff must not:

- Invite existing students at the College to become their 'friends' on Facebook **(or similar on other social network sites)**.
- Accept invitations from existing students at the College to become 'friends' on Facebook **(or similar on other social network sites)**.
- Post any negative or inaccurate information about the College on Social Media.
- Post anything on Social Media which would reflect poorly on the College or bring the College into disrepute.
- Post any photographs or video clips of activities that take place at College or related to College activities without checking with the member of the SMT responsible for marketing (who will know whether there is permission from students for this information to be used).
- Post contact details for any member of staff or student at the College on Social Media (or any other information that might result in a breach of the Data Protection Act).
- Set up any other groups or pages relating to the College without agreement from your Head of Department or line manager, in addition to submitting a risk assessment and obtaining permission from the Deputy Principal.
- Use social media during normal working hours to socialise with friends when they should be working.

If staff become 'friends' with past students or work colleagues on Facebook (or similar on other Social Media), they should adhere to the code of conduct with regard to not bringing the College into disrepute.

Employees are advised to refrain from publishing any personal or sensitive information on Social Media.

Default privacy settings on social media may allow for some information to be shared beyond an individual's contacts. In such situations the user is personally responsible for adjusting the privacy setting for the account. When engaged in College related activity staff must review their access and privacy settings on social media to control who can access their personal information. If staff permit students to use social media for College related activity it is their responsibility to ensure that students review their access and privacy settings on social media to control who can access their personal information, and to ensure that students do not publish any sensitive or personal information.

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 this Policy and the Acceptable Use Policy for Staff and the Acceptable Use Policy for Students and Visitors.

The College uses commercial security to screen websites and filters internet access to inappropriate content, including extremist material, under the following headings:

- Violence/hate/racism
- Intimate apparel/swimsuit
- Nudism
- Pornography
- Weapons
- Adult/Mature content
- Cult/Occult
- Drugs/Illegal Drugs
- Illegal skills/Questionable skills
- Sex Education
- Gambling
- Alcohol/Tobacco
- Games
- Hacking/Proxy avoidance systems
- Personals and dating

The College will monitor and record any attempt to access the following inappropriate content and this may lead to disciplinary action. Any offence under English Criminal Law will be referred to the relevant police (or other) authorities.

It may be possible to allow access to blocked sites for the purpose of legitimate research. If a member of staff or their students needed to research blocked sites they should discuss this with their Head of Department in the first instance and seek approval from the Deputy Principal. If a member of staff considers it is appropriate for students to access or interact with potentially sensitive or extremist material as part of their studies, it is the responsibility of that member of staff to:

1. seek the agreement of their Head of Department

2. conduct a risk assessment which identifies the potential risks and appropriate controls to promote student safety
3. submits the risk assessment to and receives authorisation by the Deputy Principal for the activity or task in question

The decision to add or remove sites from the list of those filtered is taken by the Deputy Principal or e-Safety Officer in consultation with the IT Support Manager. The procedure followed is outlined in **Appendix B.**

6. Risk Assessment

In making use of external online platforms, all staff must first carry out a risk assessment for e-safety **(See appendix G).** A risk assessment must also be carried out where a student is researching a topic that may contain extremist material or conducting an activity that involves safeguarding concerns, including e-safety. All forms must be submitted to the e-Safety Officer for consideration and approval.

For examples of questions that might be included, refer to the JISC Legal Web 2.0 Tutor's Checklist.

7. Behaviour

The College will ensure that all users of technologies adhere to the standard of behaviour as set out in the Code of Conduct for Staff and Acceptable Use Policy for Staff and/or the Code of Conduct for Students and the Acceptable Use Policy for Students and Visitors.

The college will not tolerate any abuse of IT systems. Whether offline or online, communications by staff and learners 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 Code of Conduct for Students and/or Code of Conduct for Staff.

Where conduct is considered illegal, the college will report the matter to the police.

8. Communications

The College requires all users of IT to adhere to the Acceptable Use Policy for Staff and/or the Acceptable Use Policy for Students and Visitors which states clearly when email, mobile phones, social media sites, games consoles, chatrooms, etc. may be used during the college day

9. Use of Images and Video

The use of images, or photographs, is encouraged in teaching and learning 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 learners where consent has been given.

Staff must not copy, download, share or distribute photographs or images online without permission from those whose image they wish to use. Approval must also be given by the Principal, and staff must submit their request to the Personal Assistant to the Principal.

Approved and published photographs must not include names of individuals without consent.

10. Personal Information

The College regularly collects and stores the personal information of students and staff e.g. names, dates of birth, email addresses, assessed materials and so on. College staff must keep personal information safe and secure and express permission is required from a student if personal information is to be shared with a third party.

Staff must not post their own personal information, or that belonging to others, to the college website without the permission of those concerned in addition to approval by the Principal, and staff must submit their request to the Personal Assistant to the Principal.

Staff must keep learners' 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 must log off on completion of any activity, or where they are physically absent from a device for any period.

All mobile devices (belonging to the College or the personal devices of staff) which contain personal information must be password protected and/or encrypted.

Where the personal data is no longer required it must be securely deleted.

Please see the Staff Guide to Keeping Personal Data Safe (Appendix C) for the practical steps staff must take to keep personal data safe. Staff should also consult the College's Data Protection Policy.

11. Education and Training

With the current unlimited nature of internet access, it is impossible for the college to eliminate all risks for staff and students. It is our view therefore, that the college should support staff and students stay e-safe through helping them develop the skills to be able to identify and manage risks effectively.

Students

Issues associated with e-safety apply across the curriculum and Students will receive guidance on what precautions and safeguards are appropriate when making use of the internet and technologies in relation to their subject(s) and as part of the tutorial programme. To this end all students will conduct a research based activity each year through which they will identify possible risks and the strategies to manage them. 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. 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. It is expected that subjects that involve students in frequent internet research, or activity that is likely to involve greater risks regarding e-Safety will ensure their students have further opportunities to learn how to identify and manage the e-Safety risks.

Further guidance on how to use the internet safely will be given to students when they log on to the college network, through posters and leaflets, and via the College Gateway.

See Appendix H for the Student Guide to Using the Internet Safely

Staff

All staff will have e-safety training led by the e-Safety Officer and Designated Lead for Safeguarding as part of and in accordance with the College's programme of Safeguarding training. Staff must agree to the College's Acceptable Use Policy for Staff prior to using the College IT systems. Updates will be provided via staff, department and subject meetings.

Any new staff or volunteers will receive training on the college IT system, led by the e-Safety Officer. They must also agree to the College's Acceptable Use Policy for Staff.

12. Incidents and Response

Where an e-safety incident is reported to the college this matter will be dealt with seriously. The college will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring.

Students must report any concerns or incident to the College e-Safety Officer and Designated Safeguarding Lead, or to their teacher, tutor, Head of Year or member of the Senior Management Team.

Staff must report any concerns or incident to the College e-Safety Officer their line manager as soon as possible. Following any incident, the college will review what has happened and decide on the most appropriate and proportionate course of action.

Where the incident or concern is in relation to cyber bullying the appropriate Head of Year will investigate and determine the appropriate response by the College in consultation with the e-Safety Officer as appropriate, and in a manner consistent with the Student Code of Conduct.

Where the incident or concern is one in relation to a general e-Safety issue the e-Safety Officer and Designated Safeguarding Lead will determine the appropriate response by the College in consultation with members of the College e-Safety Group or College Principal and other members of the Senior Management Team as appropriate.

The College's response, including any sanctions, will be in line with the college Acceptable Use Policy for Staff and Code of Conduct for Staff and/or the Acceptable Use Policy for Students and Visitors and Code of Conduct for Students. Serious incidents will be dealt with by senior management, in consultation with appropriate external agencies.

13. Feedback and Further Information

The College welcomes all constructive feedback on this and any other college policy. If you would like further information on e-safety, or wish to send us your comments on our e-Safety Policy, then please contact the e-Safety Officer and Designated Safeguarding Lead Ruth Scotson ruth.scotson@wsfc.ac.uk.

14. Monitoring

The policy will be reviewed annually by SMT.