E-Safety Policy

2018-20

Responsible Officer:	Head of Learning Technology, Learning Centres & CPD
Date of issue:	September 2018
Next review date:	September 2020
Procedure available:	Staff Intranet & VLE
Policy Authorised by:	Executive

E-Safety Policy

Introduction:

Buckinghamshire College Group 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 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, training, guidance and implementation of our policies. In furtherance of our duty to safeguard students, we will do all that we can to make our students and staff stay safe online and to satisfy our wider duty of care.

Scope:

The policy applies to all students and 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 and accept the Acceptable Use Agreement. The e-Safety Policy applies to all use of the internet and forms of electronic communication such as email, mobile phones, social media, instant messaging etc.

Definition:

The term e-safety is defined for the purposes of this document as the process of limiting the risks to children, young people and vulnerable adults when using Internet, Digital and Mobile Technologies (IDMTs) through a combined approach to policies and procedures, infrastructures and education, including training, underpinned by standards and inspection.
E-safety risks can be summarised under the following three headings:

Content

- Exposure to age-inappropriate material
- Exposure to inaccurate or misleading information
- Exposure to socially unacceptable material, such as that inciting violence, hate or intolerance, sites promoting radicalisation or pornography
- Exposure to illegal material, such as images of child abuse
- Illegal Downloading of copyrighted materials e.g. music and films

Contact

- Grooming using communication technologies, potentially leading to sexual assault, child sexual exploitation and radicalisation
- The use of assumed identities on gaming platforms
- Bullying via websites, mobile phones or other forms of communication device
- Spyware, e.g. use of Remote Access Trojans/Tools to access private information or spy on their victim.

Commerce

- Exposure of minors to inappropriate commercial advertising
- Exposure to online gambling services
- Commercial and financial scams

Responsibilities

The Head of Learning Technology, Learning Centres & CPD and the Safeguarding and Prevent Officer are responsible for maintaining this policy.
The following are responsible for implementing it:-

- The Safeguarding and Prevent Officer is responsible for keeping up to date with new technologies and their use, as well as attending relevant training. They will deliver staff development and training, record incidents, report any developments and incidents and liaise with the local authority and external agencies to promote e-safety within the College community. The Safeguarding and Prevent Officer will also provide pastoral and practical support for students dealing with issues related to e-safety.
- The Executive Director of Human Resources for all e-safety matters in relation to College staff.
- The Head of Information & Technology for championing good e-safety practice in College IT facilities and processes, and for providing technical expertise when issues are being investigated.
- The Head of Student Services for incorporating e-safety into student induction and delivering e-safety as part of the Tutorial Scheme of Work.
- All tutors for embedding e-safety education and practice into their teaching programme.
- All College Managers for implementing good e-safety practice and safeguards consistent with this policy in their area of responsibility.
- The College Safeguarding Committee for overseeing and reviewing e-safety arrangements.
- All members of College staff for staying alert to and responding appropriately to any potential or actual e-safety issue.

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 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 Acceptable Use Policy.
The College complies with guidelines set out by the Counter Terrorism Internet Referral Unit (CTIRU) and has a statutory duty to ensure their systems cannot be used to access any of the websites on the CTIRU list.

Behaviour

Buckinghamshire College Group will ensure that all users of technologies adhere to the standard of behaviour as set out in the Acceptable Use 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 procedures.

Use of Images and Video

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 (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 and staff should receive training on 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. Buckinghamshire College Group teaching staff will provide information to students on the appropriate use of images as detailed in the Acceptable Use Policy. This includes photographs of students and staff as well as using third party images. Our aim is to reinforce good practice as well as offer further information for all users on how to keep their personal information safe. No image/photograph can be copied, downloaded, shared or distributed online without permission from the owner. Photographs of activities on the College premises should be considered carefully and have the consent of the Marketing department before being published. Approved photographs should not include names of individuals without consent.

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 to stay e-safe through regular training and education. This will provide individuals with skills to be able to identify risks independently and manage them effectively.

For students:

Students have access to e-safety e-learning modules and assessments and 16 -18 full time students will attend e-safety tutorial sessions. An area on the VLE has also been set up with e-safety resources which are signposted at induction. 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.

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. Appendix A shows E-Safety Guidelines and Appendix B shows Guidelines for Students (Social Media)

For staff:

Staff will take part in mandatory Safeguarding training (which includes e-safety) with updates every 3 years. This will be led by the Safeguarding and Prevent Officer and will take the format of a workshop, allowing teachers hands-on experience. Further resources of useful guidance and information will be issued to all staff following the session. Staff attendance is recorded and monitored by the Professional Development Administrator and HR.

Staff will also be asked to sign the College (staff) Acceptable Use Policy. Appendix A shows E-Safety Guidelines and Appendix C shows Guidelines for Staff (Social Media).

Incidents and Response

Where an e-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 tutor, Duty Manager or to the College Safeguarding and Prevent Officer. Where a member of staff wishes to report an incident, they must contact 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. 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. The College VLE also displays the CEOP reporting functionality where students and staff can report online abuse.

Checklist:

Impact on Students/Staff: Provide College students and staff members a safe online environment.
Impact on Diversity: This is an inclusive policy and covers e-safety issues involving hate and intolerance.
Impact on PREVENT: This policy highlights the dangers of radicalisation through websites and social media
Impact on Health & Safety: Provide a safe online environment for Staff and Students
Impact on Data Protection/Freedom of Information: Outlines staff and student guidelines for protection of personal data online
Link with Strategic Plan: Helping to achieve excellence
Communication/Consultation Plan: This Policy is reviewed by the Safeguarding Committee and posted on the VLE and Intranet.
Process of review: Policy is reviewed annually
Process of review of effectiveness: As above
Legal authority:

- Racial & Religious Hatred Act 2006
- Sexual Offences Act 2003
- Police & Justice Act 2006
- Computer Misuse Act 1990 (s1-3)
- Communications Act 2003 (s127)
- Data Protection Act 1998
- Malicious Communications Act 1988 (s1)
- Copyright, Design & Patents Act 1988
- Public Order Act 1986 (s17-29)
- Protection of Children Act 1978 (s1)
- Obscene Publications Act 1959 & 1964
- Protection from Harassment Act 1997
- Regulatory of Investigatory Powers Act 2000

Responsibility for maintaining this policy rests with: Head of Learning Technology, Learning Centres & CPD
Links to other policies:
Acceptable IT Use Policy – Staff
Acceptable IT Use Policy – Learners
Digital Learning Strategy
Social Media Reputational Management Policy
Academic Misconduct Policy
Learner Disciplinary Procedure
Communications Strategy
Employee Code of Conduct
Safeguarding Children and Young People Policy
Safeguarding Vulnerable Adults
Prevent Policy
Anti-Bullying Policy

Appendix A - E-Safety Guidelines

- Keep your personal information private – avoid sharing personal information such as your phone number, home address or photographs with people you don't know in person and trust.
- Check whether the social media networks you use allow you to create friend lists. These lists let you manage who sees what. For example, you may only want your closest friends to see some information.
- Use private messages for people you know in person and trust; be careful of private messaging people you don't know.
- Use a strong and unique password for all of your online accounts – a combination of letters, numbers and symbols (and if you've ever shared it in the past, CHANGE IT).
- Know how to block someone if they make you feel uncomfortable or upset.
- Learn how to save chat logs and texts so that if someone does make you uncomfortable or upset, you have evidence to report them.
- Remember to log out of a site properly after use, especially on a shared computer.
- Keep your clothes on when using webcam – images of you could end up in the wrong hands!
- Think very carefully about meeting someone face to face who you only know online – NEVER do this alone, always talk to your parents or carers before you go ahead with this and take a trusted adult friend along with you.
- Students or staff should report any abusive behaviour immediately to the Safeguarding and Prevent Officer on the confidential helpline, Amersham – 07772 893482, Aylesbury – 07920 072463, Wycombe – 07772 893257 or email confidentialhelpline@buckscollegegroup.ac.uk

Appendix B – Guidelines for Students (Social Media)

As part of our duty of care to our students, the College sets out guidelines, below, for students when using social media. These guidelines are included in the student handbook and the purpose of including them here is to make staff aware of the guidelines and to encourage staff to discuss them with students.
Students should follow the guidelines below at all times:

- Do not enter into a "friends" relationship online with someone you do not know
- Do not use social media to harass, threaten, insult, defame or bully another person or entity; to violate any College policy; or to engage in any unlawful act, including but not limited to gambling, identity theft or other types of fraud
- Do not access or participate in social media which insights hatred or promotes radicalisation.
- Set up privacy settings carefully, ensure you are not sharing any information that you do not want to and check these on a regular basis
- Participating in social media use as part of a College or course activity is optional. Students may opt out at any time
- Discussions on Buckinghamshire College Group branded social media should be appropriate and College or Course related
- When posting on sites linked to Buckinghamshire College Group or when mentioning or referring to Buckinghamshire College Group on social media do not:
    - Use foul or abusive language
    - Harass, threaten, insult, defame, blackmail or bully another person
    - Refer to any other member of the Buckinghamshire College Group community, whether student or staff, in a derogatory or insulting manner

    - Refer to the College, its courses or facilities or any other aspect of its offering, in a derogatory or insulting manner
    - Post or comment in any way that reflects poorly on the College or is deemed to interfere with the conduct of College Business
- Posting of messages that are deemed inappropriate will be dealt with under the student disciplinary procedure
- Copies of inappropriate posts may be reported to parents/ guardians and the appropriate authorities. Before you post a message, think carefully about its content and ask yourself how you would feel if you received that message or know that it may be disclosed in court
- Any form of abuse or cyber-bullying will be dealt with under the student disciplinary procedure
- Students should report any abusive behaviour immediately to the Safeguarding and Prevent Officer on the confidential helpline, Amersham – 07772 893482, Aylesbury – 07920 072463, Wycombe – 07772 893257 or email confidentialhelpline@buckscollegegroup.ac.uk

Appendix C – Guidelines for Staff (Social Media)

This policy sets out guidelines for staff, below, for the use of social media. These guidelines apply to: Posting to any Buckinghamshire College Group social media site; communicating with members of the Buckinghamshire College Group community including staff or students; discussing the College on any site; whether at College and using the College network and equipment or through a personal account or using a personal phone, computer or other device from any other location.
Staff should follow the guidelines below at all times:

- Be professional; as a Buckinghamshire College Group employee you are an ambassador for the organisation. Protect the Buckinghamshire College Group brand and values at all times, do not make derogatory comments about Buckinghamshire College Group products, services, management, employees or systems
- Never have a “friend” relationship with a student online, where personal details are shared
- If the Social Media requires a login, create a separate “work” login and ensure any privacy settings are set appropriately so that no personal information can be viewed.
- Staff should not share any personal information online including home address, personal telephone numbers, personal email addresses or date of birth
- Discussions on social media sites linked to Buckinghamshire College Group should be appropriate and be College or Course related
- When using Facebook (in line with the Social Media Reputational Management Policy), Pages are permitted and monitored by the Marketing department. Groups are not permitted, online discussion and communication should take place on College systems (e.g. Cloud) which are closely monitored.
- When communicating with students who are under 18 via email, where possible, College student email addresses should be used.
- Email communications with students under 18 must happen within normal working hours (8.30 – 5pm).
- Staff should not comment on anything related to legal matters, litigation, or any parties the College may be in dispute with or anything that may be considered a crisis situation.
- Do not access or participate in social media which insights hatred or promotes radicalisation.
- Do not upload to video/photo sharing sites (e.g. YouTube) unless it is done via the Buckinghamshire College Group official channel. Contact Marketing to do this
- Do not post a person’s photograph or video image without first obtaining permission and signed release forms from anyone depicted in the photograph or video (any photographs of children and young people under the age of 16 should have parental permission) Blank release forms may be requested from the Marketing team and should be promptly returned after they are signed

- Protect confidential and sensitive information at all times (e.g. referring to sickness absence of others etc.)
- Whenever appropriate, link back to information posted on the College website instead of duplicating content. For assistance with linking to the website please contact the Marketing team
- Remember that statutory regulations and Buckinghamshire College Group policies including inappropriate conduct such as sexual (or other) harassment, bullying, discrimination, defamation, infringement of copyright and trademark rights, data protection and unauthorised disclosure of student records and other confidential and private information, will apply to communications by Buckinghamshire College Group students and staff through social media
- When posting on sites linked to Buckinghamshire College Group or when mentioning or referring to Buckinghamshire College Group on social media do not:
    - Use foul or abusive language
    - Harass, threaten, insult, defame or bully another person
    - Refer to any other member of the Buckinghamshire College Group community, whether student or staff, in a derogatory or insulting manner
    - Refer to the College, its courses or facilities or any other aspect of its offering, in a derogatory or insulting manner
    - Post or comment in any way that reflects poorly on the College or is deemed to interfere with the conduct of College business
- Staff should not spend an excessive amount of time while at work using social media websites in a personal capacity. They should ensure that use of social media does not interfere with their other duties as this is likely to have a detrimental effect on productivity
- Any breach in this Policy could result in an investigation and disciplinary procedures under the staff disciplinary policy. Serious breaches of this policy, for example incidents of bullying of colleagues or social media activity causing reputational damage to the College, may constitute gross misconduct and lead to dismissal.
- Staff should abide by the Guidelines on Professional Boundaries and Standards.