KMS 452 eSafety Policy

KMS 452 Appendix A – Social Media Policy for Students

To be read in conjunction with:

KMS 004H Student Code of Conduct
KMS 017A Student Disciplinary Code of Conduct
KMS 250 Safeguarding Policy
KMS 257 Anti Bullying Policy
KMS 251 Prevent Policy
KMS 260 Student / Parent Code of Conduct
KMS 400 Equality Policy
KMS 450 ICT Acceptable Use Policy – appendix ? and ? Students and Staff
KMS 451 Bring Your Own Device (BYOD) Policy
KMS 600 Staff Code of Conduct
KMS 860 Data Protection (GDPR) Policy

Introduction

Kingston Maurward College recognises the benefits and opportunities which all new technologies offer to teaching and learning.

We provide internet access to all students, apprentices, staff and visitors to 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.

Such communication methods can increase the risk of misinformation, inappropriate communication, unprofessional behaviour and negative impact and it is therefore essential that there should be a policy in place in order for the College to fully embrace new methods of communication for 21st century educational delivery.

The College's approach is to implement appropriate safeguards while supporting staff and students to identify, consider 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 safeguarding responsibilities to all students and apprentices, we will do all that we can to make sure all members within the College community can stay e-safe and to satisfy our wider duty of care.

Purpose

The purpose of this policy, and any resulting appendices and processes, is

- to ensure the safety and wellbeing of young people and the wider College community is paramount when using the internet, social media platforms, using tablets, laptops, PCs, mobile devices and smart technology (via College WiFi, Network, 3G, 4G and 5G)

- to provide staff with overarching principles that guide the College's approach to online safety

- to ensure that as a College and organisation, we operate in line with our values and within the law in terms of how we use online services, devices and smart technology

Who should be aware of this Policy

All students, apprentices, parents / next of kin, staff, governors, volunteers and visitors to the College.

The policy applies to all members of the College community who have access to college IT systems, both on campus and via remote access.

This policy should be read in conjunction with the ICT Acceptable Use Policies for staff and students, and the Staff and Student Code of Conducts.

Legal Framework

This policy has been written on the basis of the legislation, policy and guidance that seeks to protect young people in England.

Summaries of the key legislation and guidance are available here

https://learning.nspcc.org.uk/child-abuse-and-neglect/online-abuse

https://learning.nspcc.org.uk/child-abuse-and-neglect/bullying

https://learning.nspcc.org.uk/child-protection-system/england

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1014224/Sexual_violence_and_sexual_harassment_between_children_in_schools_and_colleges.pdf

https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people

Roles and Responsibilities

All students must know what to do if they have e-safety concerns and who to. In most cases, this will be their Course Manager, Apprenticeship Coordinator or a member of the Student Welfare team (121@kmc.ac.uk or 01305 215121).

The College expectation is that all students will be responsible users when accessing IT equipment, systems and networks etc.

All staff are responsible for ensuring the safety of students / apprentices and should report cases appropriately.

Staff should report serious concerns to a member of the Student Welfare team, following up with a report via MyConcern, and be aware that the Safeguarding team may be asked to intervene with additional support from external agencies as appropriate.

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.

However, and in line with the College's safeguarding protocols, information should only be shared with those who need to know.

Security

The College will do all that it can to make sure the College network is safe and secure and meets the Cyber Essential standards.

The College's IT Department is responsible for ensuring security software is kept up to date, with updates regularly scheduled for College IT equipment and network.

Appropriate security measures include the use of enhanced filtering and protection of firewalls, servers, routers, workstations etc. to prevent accidental or malicious access of College systems and information.

All digital communications, including email and internet postings over the College network, will be monitored and is subject to Multi Factored Authentication (MFA) and encryption where appropriate.

Expectations and Behaviours

Kingston Maurward College will ensure that all users of technologies adhere to the standard of behaviour as set out in the Acceptable Use Policies (Staff and Student).

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 to be illegal, the College reserves the right to report the incident and any supporting material to the Police.

Personal Information

Personal information is information about a particular living person.

The College collects and stores the personal information of students and staff regularly e.g. names, dates of birth, email addresses, assessed materials etc.

The College will keep that information safe and secure and will not pass it onto anyone else without the express permission of the student or member of staff.

Staff must keep students' personal information safe and secure at all times. When using any online platform, all personal information must be password protected.

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

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 training and education.

This will provide individuals with skills to be able to identify risks independently and manage them effectively.

For Students / Apprentices:

Students will receive e-safety training as part of their group tutorial programme.

Student Welfare staff will ensure that up-to-date information and relevant activities are available to support this training.

Course Managers will deliver the College's extremism tutorial as part of this programme.

Apprentices will receive guidance on e–safety through their regular reviews.

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.

As part of their Student Welfare inductions, all students are informed of how to report e-safety concerns.

For staff:

E-safety training for staff is incorporated into the College's Safeguarding training that all new staff receive at induction.

Keeping Children Safe in Education responsibilities are refreshed annually.

Safeguarding training is reinforced at least every three years when staff are required to undertake refresher training.

Key staff are required to attend update sessions every two years.

All staff receive regular safeguarding updates annually by different methods.

All staff are required to undertake appropriate training in relation to the Prevent agenda.

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 / apprentice wishes to report an incident, they can do so to their Course Manager, Apprenticeship Co-ordinator or to a member of the Student Welfare team.

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 and / or the matter may be resolved internally depending on the nature and seriousness of the incident.

Concerns or incidents relating to extremism must be reported to a member of the Safeguarding team and will then be referred, if appropriate, to the Channel process through the Prevent Referral Unit at Dorset Police.

Extremism and Radicalisation

Many extremist groups such as far right groups, animal rights activists and religious fundamentalists who advocate violence or other criminal activity, use the internet as a means of recruiting young / vulnerable people.

Because of their personal circumstances, some young / vulnerable people may be susceptible to these influences.

Staff should remain vigilant to those young / vulnerable people who are in danger of being targeted by or exposed to harmful influences from violent extremists via the internet.

Young / vulnerable people should be warned of the risks of becoming involved in such groups and it should be against service policy to access such sites.

Guidance on staying safe online for Students / Apprentices

Personal Safety

- Don't post any personal information online – like your address, email address or mobile number
- Think carefully before posting pictures or videos of yourself. Once you've put a picture of yourself online most people can see it and may be able to download it - it's not just yours anymore
- Sexting images of yourself, even to someone you trust, is dangerous as they could still end up being posted on the internet and going viral
- Keep your privacy settings as high as possible
- Keep your username and password secure; it is recommended that you use three random words, including a mix of capital letters, numbers and special symbols
- Never give out or share your passwords
- Don't befriend people you don't know
- If you meet up with someone you have met online, arrange to meet them in a public place and tell someone where you are going and what time you expect to be back. If possible, take a friend with you

- Remember that not everyone online is who they say they are

- Be careful about joining organisations or groups without checking them out first. They may appear to be well-meaning but they could be trying to engage you in illegal or dangerous activities – for example, some political, religious or animal rights groups may want you to break the law in the name of their cause

- Don't put anything online that you might later regret - remember that the internet has a long memory and things you share now may have the potential to cause you embarrassment or distress in the future

- If you see something online that makes you feel uncomfortable, unsafe or worried: leave the website, turn off your computer if you want to and tell someone immediately

  You can report it to your Course Manager, Apprenticeship Coordinator or a member of the Student Welfare team

Responsibilities towards others

- Think carefully about what you say before you post something online

- Be polite and responsible when you communicate with others. Do not use strong, aggressive or inappropriate language

- Respect other people's views even if you don't agree with them

- Don't take photographic images and/or audio recordings of anyone or distribute them without their express permission

- Don't ask to use someone else's password details

- Make sure that you comply at all times with the Acceptable Use Policy for Students which can be found on the Student Moodle Portal – KMC Documents

Guidance on staying safe online for staff

- All digital communications with students must be professional at all times

- Personal information, including contact information, should not be shared with students, parents or next of kin

- Don't post anything that may compromise your professional role or bring the College into disrepute

- Only use social media sites with students that are authorised by College. Make sure that at least one other member of staff has access to the forum you are using

- Don't befriend or communicate on social networking sites with students[1] or their parents / next of kin - keep work and home separate

If you are a manager or supervisor, avoid being friends with employees

- Avoid texting / messaging – both can be manipulated and students / apprentices should not have access to your personal mobile number

- Use College equipment if taking photos and be aware of posting photos publicly. You must seek students'/ apprentices' permission before posting photos, even on a College Facebook page

- Avoid taking photographs or videos in a one-to-one situation and remember that you may be asked to justify any images in your possession

- Don't put anything online that you might later regret – remember that the internet has a long memory

- Report any concerns so that they can be dealt with openly and effectively. You can refer them to your line manager, the Deputy Principal or the Assistant Principal Student Experience & Progression

- If you are shown images that concern you, do not copy, print, download or forward those images – seek further guidance

- Make sure that you comply at all times with the Acceptable Use Policy for Staff

- Report concerns about students or other staff to the Safeguarding team if you believe that they are at risk of sexual grooming, bullying, sexting or radicalisation

- Remember that education is key - help your students / apprentices to be aware and stay safe online

---

[1] If your child has friends who may be students at KMC, restrict your privacy settings so that his/her friends cannot see your pages and you cannot see the friends' pages

KMS 452 Appendix A

Use of Social Media Policy for Students

The purpose of this policy statement is to ensure that all users of social networking media (for example, but not limited to: Facebook, Instagram, LinkedIn, Snapchat, Twitter, Tumblr, Tik-Tok, WhatsApp and You Tube etc.) are aware of the parameters of what the College deems to be acceptable and unacceptable use and acts accordingly within these guidelines.

The College's definition of social media in this context is as follows:

'the opportunity to use instantaneous channels for information sharing and communication through social networking platforms. Social media can include the use of text, audio, video, images, podcasts and other multimedia communications'

It also includes the College's own internal email system and Microsoft Teams.

The College recognises that students will inevitably make use of social media and networking sites within their own personal lives away from the College environment, as well as seeking to embrace the use of these technologies for their College activities, where appropriate.

This statement exists to support the appropriate use of these technologies for specific purposes and exists for the protection of both staff and students and reputation of the College.

It therefore designed to be clear and explicit about appropriate behaviour.

Students using Social Media platforms to interact should also note the requirement to protect the privacy and well-being of all members of the College community at all times, as well as The College's brand, image, ethos and reputation in all associated activities, i.e. educational (Apprenticeships, FE and HE, Short-Course and Adult Education) and commercial activities.

It is the College's opinion that all information posted on the internet using social media technologies, will be considered as *'published, permanent and potentially public'*, even if a user may deem it to be *'protected'* in some way.

Similarly, any information posted on any of the College's internal communication systems (i.e. email and Microsoft Teams etc.) will be considered as *'published, permanent and potentially public'* to all authorised users of these systems.

By definition, social media technologies are designed to enable quick and simple ways of sharing information; therefore, it is open to easily, and potentially inadvertently, sharing information to a wider audience than a person may originally intend.

It should also be noted that seemingly innocent information such as photographs, videos, opinions or comments are open to misrepresentation and unauthorised distribution.

Student Conduct

All students and apprentices are expected to abide by the College's expectations of conduct and any associated policies.

All members of the College community are expected to respect the rights and privacy of peer students, apprentices and staff, as well as the reputation of the College.

All students

- are considered to be responsible for their behaviour when using the internet, including their use of social media platforms, games and apps; this includes the resources they access and the language they use

- are required to not deliberately browse, download or upload material that could be considered offensive or illegal; if a student accidently comes across such material they are required to report it to a member of staff or the IT Team for assistance

- are encouraged to think carefully about how they express themselves, and bear in mind the need to safeguard themselves

- Material posted on the internet can be hard to delete; any forms of content posted or shared is to be considered as permanently available for review.

Where students make use of social media and networking technologies (including both internally and externally hosted sites) it is expected that they should not post comments or any other type of material on a social networking site, blog, or send text messages / digital messages that:

- could be viewed as threatening, bullying / harassing, offensive or illegal to another member of the College community

- may be interpreted to be racist, homophobic, sexist, ageist or otherwise discriminatory about another member of the College community

- are counter to the College's Equality and Diversity Policy or IT Security Policy

- contains language, sound, images or video which may cause offense to another member of the College community

- expresses opinions or encourages other members of the College community in the incitement of violence, extremism or to break the law

- are considered likely to bring the College into disrepute

The College will consider seriously any incidents where students have, or are deemed to have, broken these guidelines. Appropriate action and sanctions will be

taken in line with the College's Student Disciplinary Code of Conduct, up to and including a recommendation to the Principal for permanent exclusion.

The College also reserves the right to report incidents and any associated content to the Police when it considers this to be an appropriate action.

Monitoring Online presence

The College reserves the right to monitor the student's use of the internet, when connected to the College's Wi-Fi and network via College or personal devices, all student email traffic and Microsoft TEAMs communications.

Students should be aware that all use of the College systems is governed by the Acceptable Use Policy and the College Email and IT Security Policies and processes.

It should be noted that the College reserves the right to amend this policy at its discretion and in line with incident management, College needs and to ensure its relevance to technological developments is maintained.