Social Media Policy

Policy Statement
Al-Maktoum College recognises the benefits and opportunities that social media can bring as a tool. For the purposes of this policy, social media is defined as a type of interactive online application that allows parties to communicate instantly with each other or to share data in a public forum. This includes online social forums, anonymous apps, blogs, video-and image-sharing websites and similar facilities.

It can be used to share news, information and successes, keep staff and students up to date with important developments and promote healthy academic debate about controversial subjects and areas of research.

However, there are also a number of risks associated with the use of social media which could ultimately impact on the College's reputation, so employees must be aware of the potential impact on both themselves and the College.

Aim
This policy is intended to minimise the risks of social media which can negatively impact on the wellbeing of students and staff and the reputation of the College, so that students and staff can enjoy the benefits of social networking, whilst understanding the standards of conduct expected by the College.

Scope
This policy relates to all employees who create or contribute to blogs, wikis, social networks, apps, forums, virtual worlds, or any other kind of social media. It applies to all users and all forms of social media where there is potential impact on the College, whether for work-related or personal use, whether during working hours or otherwise, whether social media is accessed using the College's IT facilities and equipment, or equipment belongs to members of staff or any other third party.

Legal Risks
There are a number of legal risks relevant to the use of social media and, staff and students using social media should be mindful of these, in particular:

- Defamation
- Intellectual property infringement
- Breach of confidence
- Harassment

Social Media Account Management
All corporate social media accounts must adhere to the College's brand guidelines and the account profile information should clearly state the purpose of the account and the hours during which it is monitored. It is important that all social media accounts are kept up to date, posted from regularly and monitored on a frequent basis. Questions should be responded to promptly within operating hours.

Where several members of staff require access to the same social media account, there must be an agreed overall account manager.

Users of the College's social media accounts are responsible for keeping passwords secure and of adequate strength. Where possible two factor authentication should be used. Passwords should not

be shared. The account managers or Communications Officer should maintain a list of social media platforms being used by the College and a list of users. Leavers should have their access removed or password changed.

Social Media Posts
All posts from corporate social media accounts represent the College. It is vital that messages posted are carefully considered, appropriate and do not damage the reputation of the College or otherwise bring it into disrepute. Safeguards should be put in place to minimise the risk of communication errors via social media, including checking content with the Communications Officer before publishing.

Content posted or promoted on corporate accounts must be respectful of others and courteous. Corporate accounts must not be used to criticise or argue with colleagues, students, customers, partners or competitors.

It is also important that content is accurate and does not commit to something which the College does not intend to deliver. If a mistake is made, it is important to be transparent and update the page with a correction.

Social Media Conduct
Staff are personally responsible for what they communicate on or through social media and they must adhere to the standards of behaviour set out in this policy. Staff have a responsibility to represent the College accurately and fairly in any online space and are expected to uphold the values of the College. Use of social media must not infringe the rights, or privacy, of staff, students and/or third parties.

There should be no expectation of privacy or confidentiality in anything you create or share on social media platforms. When you create or exchange content using social media you are making a public statement. As such, your content will not be private and can be forwarded to third parties without your consent. You should therefore consider the potential sensitivity of disclosing information. Once sensitive or confidential information (or offensive or defamatory information) has been disclosed, it cannot be recovered and this may result in liability both for the College and also you personally.

Individuals' Personal Social Media Accounts
Social media can be an important tool for colleagues' professional activity and provide a helpful platform for profile raising and enhancing networks. It is recommended that staff using social media for both professional and personal reasons maintain separate accounts for these purposes as the audiences for each activity are often distinct.

Individuals' personal accounts should not use the College's branding and if staff do discuss their work on social media, they should make it clear on their profile statement or elsewhere that the views expressed are their own and do not necessarily reflect those of the College. All employees should consider what they are posting on their individual accounts.

The College does not and will not monitor individuals' accounts. However, if a concern is raised regarding content posted on a staff member's social media account and the post is considered to be misconduct (as defined in the College's Disciplinary Procedure), the College has the right to request the removal of content. In addition, the matter may be addressed through the College's Disciplinary Procedure. Serious breaches including, but not limited to, harassment or bullying of colleagues and the misuse of confidential information may constitute gross misconduct and may lead to action including dismissal.

The policy should be read in conjunction with the Data Protection Policy.