UBL SOCIAL MEDIA POLICY

1. RATIONALE

A policy is required to have an overarching document defining the roles and responsibilities of various stakeholders of the bank in relation to social media usage.

2. OBJECTIVE

This policy is intended to help employees of United Bank Limited ("UBL") make appropriate decisions about the use of social media such as Twitter, Facebook, WhatsApp, YouTube, Google and LinkedIn and includes other social media but is not exclusive to blogs, video, picture blogging and audio.

The principles of this policy apply to use of social media regardless of the method used to access it - it covers static and mobile IT/computer equipment, as well as work and/or personal smartphones etc.

The extent of this policy applies to UBL employees acting in their capacity as staff/representatives of the Bank. It covers any and all comments, posts, visuals, videos, etc. they may have posted on the social media which associate them in any way to the Bank, whether through something said, shown or implied. Personal posts of employees as individuals are only covered up to the extent of their association to UBL in any way.

3. SCOPE

This policy outlines the standards UBL requires its staff to observe when using social media, and the action that will be taken in respect of breaches of this policy. The principles of this policy apply to use of social media regardless of the method used to access it. Although the same principles and guidelines that apply to employees' behavior in general, apply to activities online as well but due to the nature of internet and its widespread use, more accountability is to be expected.

This policy supplements other related guidelines and policies such as UBL's intranet policy, e-mail policy, Social Media Guidelines and the Code of Conduct.

4. APPLICABILITY

This Policy comes into force at once and will remain valid for a period of three years from approval date. It covers all employees of the Bank, both in Pakistan and abroad, in the management as well as non-management cadre, directors, contractual staff (full time or part time) either on Bank contract or employed through third party, and trainees (collectively referred to as 'employees' in this Policy).

5. POLICY CUSTODIAN

The Head of Marketing, currently designated as Head, Corporate Affairs & Marketing will be the custodian of this policy and will be responsible for the review and update of the policy document prior to expiry.

6. RESPONSIBILITY(S) OF BOD AND SENIOR MANAGEMENT

The BoD has the final authority to approve the Policy as recommended by Senior Management (or approve any amendments thereof) and is also responsible for overall oversight for implementation of this policy across the organization through Senior Management.

7. RESPONSIBILITY FOR IMPLEMENTATION OF THE POLICY

The Corporate Affairs & Marketing Department ("**CAM**") has overall responsibility for the effective operation of this policy. However, all staff are responsible for their own compliance with this policy and for ensuring that it is consistently applied. All staff should ensure that they take the time to read and understand it.

Questions regarding the content or application of this policy should be directed to Head Corporate Affairs & Marketing.

8. SOCIAL MEDIA INTRODUCTION

Since the term social media is used in a number of different ways, it is important to understand what is being meant by Social Media in the context of this policy. Social media is any tool or service that facilitates conversations over the internet. Social media applies not only to traditional big names, such as Facebook, Twitter, Instagram, YouTube and Tiktok, but also applies to other platforms being used that include, which an employee might not consider as Social Media. Platforms such as, Pinterest, Flickr, Quora, Tumblr, Reddit, Snapchat, Snack Video, online forums, blogs and wikis are all part of social media.

9. PERSONAL USE OF SOCIAL MEDIA

Personal use of social media in the workplace through hand held devices or through intranet is subject to certain conditions, as detailed below.

- use must be minimal and take place substantially outside of normal working hours, for example, breaks, lunchtime.
- use must not interfere with business or office commitments

Employees are also personally responsible for what they communicate on social media sites **outside the workplace**, for example at home, in their own time, using their own equipment. Employees must always be mindful of their contributions and what they disclose about the Bank. For further details, see Point 10, 'General rules for social media use' below.

10. GENERAL RULES FOR SOCIAL MEDIA USE

Whenever an employee uses social media, he/she must adhere to the following general rules. The same rules would also apply when using social media outside of work:

- Employees are generally encouraged to use social media for constructive and value addition purposes. Our organization trusts and expects employees to exercise personal responsibility whenever they are using social media, which include not violating the trust of those with whom they are engaging.
- Employees should not post or forward a link containing any abusive, discriminatory, harassing, derogatory, defamatory or inappropriate material/contents.
- Employees are personally responsible for content they publish. They should be aware that it will be public for many years.
- When using social media for personal use, employees should use a disclaimer, for example: 'The views expressed are my own and don't reflect the views of my employer'. Employees should be aware though that even if they make it clear that their views on such topics do not represent those of the organization, their comments could still damage UBL's reputation. Once an employee has disclosed his/her affiliation as an employee of UBL then they must ensure that their profile and any content they post are consistent with the professional image they present to client and colleagues.
- Employees should neither claim nor imply that they are speaking on behalf of the Bank. Only those officially designated by the President for this purpose can use social media to speak on behalf of the Bank in an official capacity.
- Employees should not post or forward any of the Bank's internal communication, circulars or other information which is not approved to be made public by the Bank. Contents pertaining to sensitive company information (particularly those found within UBL's internal networks) should not be shared to the outside online community. Divulging information like the Bank's strategic plans, internal operations, forecasts, future promotional activities, legal matters, penalties imposed by regulator and information which are commercially sensitive, anti-competitive share price sensitive (inside information) are prohibited. If an employee is unsure whether the information they wish to share falls within one of these categories, they should discuss this with Head Corporate Affairs & Marketing.
- A member of staff who feels that they have been harassed or bullied, or are offended by material posted by a colleague onto a social media website should report the same to HR in light of UBL's Harassment at Workplace policy.
- Employees should not post material in breach of copyright or other intellectual property rights.
- Employees should be honest and open, but be mindful of the impact their contribution might make to people's perceptions of the Bank.
- Employees should avoid social media communications that might be misconstrued in a way that could damage UBL's business reputation, even indirectly.

- Employees should not post anything that their colleagues or customers, clients, business partners, suppliers or vendors would find offensive, insulting, derogatory, obscene and/or discriminatory.

11. MONITORING & BREACH

Employees should be aware that any use of social media websites (whether or not accessed for work purposes) may be monitored.

Misuse of social media websites can, in certain circumstances, constitute a criminal offence or otherwise give rise to legal liability against staff and the Bank in terms of the provisions of Prevention of Electronic Crimes Act (PECA), 2016. Complaints lodged under the aforesaid law can be investigated by the Cyber Crime Wing of the Federal Investigation Agency (FIA).

If an employee notices any use of social media by another employee in breach of this policy, he/she must report it to Head Corporate Affairs & Marketing. A process will be devised for reporting such breaches to Head CAM team for their information.

Where it is believed that an employee has failed to comply with this policy, the matter shall be handled as per requirements of the Bank's disciplinary policy / procedure. If the employee is found to have breached the policy, they will face a disciplinary penalty ranging from a verbal warning to dismissal.

The penalty applied will depend on factors such as the seriousness of the breach; the nature of the posting; the impact it has had on the organization or the individual concerned; whether the comments cause problems given the employee's role; whether the employer can be identified by the postings; other mitigating factors such as the employee's disciplinary record etc.

12. DEVIATION

Any and all deviations to the policy will require prior approval from Head Corporate Affairs & Marketing, Company Secretary and President and CEO. These approvals will be kept in record for Audit purposes.