



Social Media Policy

It is the policy of Georgia Banking Company (the “Institution”) to utilize social media as may be appropriate in its marketing and communications strategies. As such, it is the policy of the Institution to comply with all applicable laws and regulations with respect to social media either directly or indirectly. Additionally, the Institution, as a matter of best practice, shall incorporate the 2013 interagency *Social Media: Consumer Compliance Risk Management Guidance* with respect to its social media efforts.

For the purpose of this policy, social media is inclusive of any form of interactive online communication in which users can generate and share content through text, images, audio, and/or video, including but not limited to:

- Micro-blogging sites (e.g., Facebook and Twitter)
- Forums, blogs, customer review web sites and bulletin boards (e.g., Yelp, Google Reviews, GlassDoor, CFPB Complaint List, Better Business Bureau)
- Photo and video sites (e.g., Tik Tok, Meta, YouTube, and Vimeo)
- Sites that enable professional networking (e.g., LinkedIn)
- Virtual worlds (e.g., Second Life)
- Social games (e.g., FarmVille and CityVille)
- Any other formats of electronic communication that gain sufficient popularity

Additionally, for purposes of this policy, messages sent via email or text message, standing alone, do not constitute social media, although such communications may be subject to a number of laws and regulations.

Social media can be distinguished from other online media in that the communication tends to be more interactive. Social media is a dynamic and constantly evolving technology. Thus, any definition for such technology is meant to be illustrative and not exhaustive. Similarly, other forms of social media may emerge in the future that the Institution should also consider.

The Board of Directors recognizes the value-add of leveraging social media in communicating with its customers and non-customers. Being active in social media networking allows the Institution to be current and relevant while leveraging low-cost marketing tools. Social media is about building a community of advocates; it provides an opportunity to share and further the Institution’s objectives and mission to provide quality financial products and services and to promote customer education with respect to financial products and services.

Social Media Risk Areas

Title/Subject GBC Policy Manual – IT Section	Document Name Social Media Policy	Version 6.0
Owner: MWhieldon	Reviewing Committee Board of Directors	Date 04.2025
		Page 1 of 6



The Board recognizes there are certain inherent risks with respect to social media regardless of the Institution’s active participation in it. Social media poses additional legal, compliance, financial, reputational, and operational risk to any business, including the Institution. Therefore, the Board has approved this Social Media Policy to facilitate both directives and guidance to the Institution’s employees and directors (collectively, “employees”) to mitigate such risk.

Compliance and Legal Risks

Compliance and legal risk arise from the potential for violations of, or nonconformance with, laws, rules, regulations, prescribed practices, internal policies and procedures, or ethical standards. These risks also arise in situations in which the Institution’s policies and procedures governing certain products or activities may not have kept pace with changes in the marketplace. This concern is particularly pertinent to an emerging medium like social media. Further, the potential for defamation or libel risk exists where there is broad distribution of information exchanges. Failure to adequately address these risks can expose the institution or individual employees to enforcement actions and/or civil lawsuits.

Social media may be used to market products and originate new accounts. When used to do either, the Institution is expected to take steps to ensure that advertising, account origination, and document retention are performed in compliance with applicable consumer protection and compliance laws and regulations. These include, but are not limited to:

Article 4 of the Uniform Commercial Code	Fair Credit Reporting Act, including Regulation V
BSA/AML Program	Regulation X RESPA
CAN SPAM and Telephone Consumer Protection Act	Regulation Z Truth in Lending
Children’s Online Privacy Protection Act	Regulation BB Community Reinvestment Act
Deposit or Share Insurance membership requirements	Regulation CC Funds Availability
Non-deposit investment products	Regulation DD Truth in Savings
Regulation B Equal Credit Opportunity Act	Fair Debt Collection Practices Act
Regulation E Electronic Funds Transfer Act	Fair Housing Act

Title/Subject GBC Policy Manual – IT Section	Document Name Social Media Policy	Version 6.0
Owner: MWhieldon	Reviewing Committee Board of Directors	Date 04.2025
		Page 2 of 6



Gramm-Leach-Bliley Act and Regulation P	Fair Lending or other applicable laws
Unfair, Deceptive or Abusive Acts or Practices	Sections 1031 and 1036 of the Dodd-Frank Act
Section 5 of FTC Act	

The Institution will also monitor development involving such laws and regulations and any impact to its social media efforts.

Reputation Risk

Reputation risk is the risk arising from negative public opinion. Activities that result in dissatisfied consumers and/or negative publicity could harm the reputation and standing of the financial institution, even if the Institution has not violated any law. The Institution’s media activities must be sensitive to, and properly manage, the reputation risks that arise from those activities. Reputation risk can arise in areas including the following:

- Fraud and Brand Identity
- Third Party Concerns
- Privacy Concerns
- Consumer Complaints and Inquiries
- Employee Use of Social Media Sites

Response Protocols for Negative Comments

Negative comments are acknowledged in a timely and professional manner. Any complaints are addressed according to GBC’s Complaint Policy.

Operational Risk

Operational risk is the risk of loss resulting from inadequate or failed processes, people, or systems. The root cause can be either internal or external events. Operational risk includes the risks posed by a financial institution’s use of information technology (IT), which encompasses social media. Social media is one of several platforms vulnerable to account takeover and the distribution of malware. The Institution will ensure that the controls it implements to protect its systems and safeguard customer information from malicious software adequately address social media usage, including its incident response protocol regarding a security event, such as a data breach or account takeover as appropriate.

Title/Subject GBC Policy Manual – IT Section	Document Name Social Media Policy	Version 6.0
Owner: MWhieldon	Reviewing Committee Board of Directors	Date 04.2025
		Page 3 of 6



Social Media Officer Appointment

The Director of Marketing, or other Officer as designated, has been selected to engage in the use of social media on behalf of the Institution. The Director of Marketing is responsible for engaging the staff as may be necessary to develop the appropriate materials to be posted. The Director of Marketing is authorized to designate an alternate in the event of his/her absence or as may otherwise be essential to complete the duties required. Notwithstanding, marketing posts to social media concerning products, rates, or Bank promotion must be reviewed and approved by Compliance to ensure compliance with the applicable regulations prior to being posted. Posts not containing items mentioned above may be approved by the Director of Marketing or other designated Bank Officer.

It is the policy of the Institution that the Director of Marketing shall continually explore methods of electronic communication and determine which of them can be useful and cost effective in its marketing strategy. It shall then devise programs for the utilization of the electronic communication channels that it selects.

The Institution may from time to time hire a third-party to design social media campaigns after appropriate vetting. However, it is the policy of the Institution not to allow non-vetted third parties, consumer or commercial, to publish social media campaigns to the Institution’s social media accounts. Any exceptions to this policy must be approved in advance by the Director of Marketing and appropriate level of Management.

Use of Social Media

Selected employees may engage in social media activity during work time provided that such activity is directly related to their work and does not interfere with their or their co-workers’ productivity. The employees selected for this task will be informed of such approval and will be provided with the parameters of their authority and directions for seeking final approval prior to posting items.

It is further the policy of the Institution that the Director of Marketing shall monitor departmental campaigns to ensure that bank-wide social media efforts directed to individual customers and non-customers do not become disruptive to the recipient due to the frequency of Bank contacts.

The Bank may engage a Social Media firm, such as Social Assurance, to monitor social media websites for mentions of any of the Bank’s trademark names and to assist with publishing and record retention. The Compliance Department monitors all such activity which is reported to the Compliance Working Committee monthly.

Title/Subject GBC Policy Manual – IT Section	Document Name Social Media Policy	Version 6.0
Owner: MWhieldon	Reviewing Committee Board of Directors	Date 04.2025
		Page 4 of 6



In the event of comments posted by customers or non-customers regarding the Institution, all such comments must be addressed proactively and timely. Any complaints shall be addressed in accordance with the Institution’s Complaint Policy and shall be copied to the Compliance Officer. The Director of Marketing is responsible for ensuring appropriate and timely responses are provided.

Use of Social Media While Off-Duty

The Institution recognizes that its employees may engage in the personal use of social media. Employees who maintain personal websites or blogs on their own time using their own facilities must ensure that social media activity does not interfere with their employment with the Institution. The Institution generally considers off-duty social media activities to be personal endeavors. Such activities may not conflict with the Institution’s guidelines, policies, or business and as consistent with any applicable employment laws, including the National Labor Relations Act.

If an individual employee or board member utilizes social media, it is the policy of the institution that any information that you shall publish shall not contain any information about the institution acquired in the course of your work. You may state that you are an employee or board member of the institution, your position with the institution or as otherwise permitted by law.

If an employee or board member has a question about whether a social media activity, he or she is considering would violate this policy, the employee or board member is encouraged to contact the Director of Marketing, Chief Compliance Officer, or Human Resources, who will assist the employee or board member in obtaining guidance or clarification.

Employees and board members should consult the Institution’s Employee Handbook for more information.

Enforcement & Oversight

The primary responsibility for ensuring compliance with this policy and its operating procedures rests with the Board of Directors and each employee. Any change to this policy must be approved by the Board of Directors. The Board shall also review and approve this policy each year for any changes that may be necessary to ensure the Institution’s compliance and for risk mitigation.

Senior Management is responsible for ensuring appropriate directives are implemented and administered in compliance with this approved policy.

Social Media software, if used, would monitor social media websites for mentions of any of the Bank’s trademark names and to assist with publishing and record

Title/Subject GBC Policy Manual – IT Section	Document Name Social Media Policy	Version 6.0
Owner: MWhieldon	Reviewing Committee Board of Directors	Date 04.2025
		Page 5 of 6



retention. The Compliance Department monitors all such activity which is reported to the IT Committee monthly. Any violation of this policy recognized outside of any program monitoring must be promptly reported to the Director of Marketing, Chief Compliance Officer, and/or Human Resources. Due to the nature of social networking, it is essential that prompt reporting occurs to mitigate any risk to the Institution.

Training

The Institution’s Director of Marketing and Chief Compliance Officer shall coordinate with senior management to ensure appropriate training to new and existing employees.

Record Retention

The Institution shall retain evidence of compliance with this policy in accordance with the applicable regulations, including but not limited to, the Truth in Lending Act (Regulation Z), Truth in Savings Act (Regulation DD), unfair, deceptive or abusive acts or practices (UDAAP and as may be proscribed by Section 5 of the FTC Act), membership requirements (e.g., member of FDIC, as applicable), the Equal Credit Opportunity Act (Regulation B) and fair housing. Social Media software may also store historical activity and trends as well as Bank responses. Internally generated posts may also be approved and released to the social media accounts through a software program. Monthly reports of the activity on the Bank’s social media accounts are available in the IT Committee packages.

Title/Subject GBC Policy Manual – IT Section	Document Name Social Media Policy	Version 6.0
Owner: MWhieldon	Reviewing Committee Board of Directors	Date 04.2025
		Page 6 of 6