Number	POL.XGB.012		
Geography	Global		
Scope	Corporate		
Owner	Nancy Williams – Communications and Marketing department		
Reviewed By	Tim Fobes, Joe LaFleur, IT Document Review Committee. GP Governance Committee.	**Date:**	Nov 29, 2020. February 2022.
Approved By	Adam Stedham	**Date:**	March 21, 2022
Effective Date	11/29/2012		

1. Purpose

This Policy provides both specific direction and information for creating related GP Strategies Policies, Standards and Standard Operating Procedures for internal and external business communications by employees about or on behalf of the Company, to include electronic, written and verbal communications, records management, and with data storage devices.

Technological advances continue to make new means of communicating available to the Company and its employees. Traditional forms of communicating, including paper correspondence and verbal discussions by telephone, continue to be supplemented by methods which can enhance communications by transmitting and recording larger volumes of information more efficiently than traditional means. As Business Communications and record storage become more technology dependent, there is a need to inform employees and external partners and adapt Company-wide guidelines in order to ensure that the Company's professional standards, adherence to global laws, business confidentiality and personal privacy data protection are maintained by all of its employees. It is essential that even as communications technologies change that these policies and practices for business communications are applied to changing business communications technology and Company conditions.

2. Scope and Applicability

This policy applies to Business Communications between employees, and between employees and third parties, to include the public media sector when applicable, by means of: telephones, fax machines, computers devices of all types and brands, computer networks, internet services, visual and verbal recordings, business systems and similar existing or future systems and means of communicating, and to the data transmitted and/or stored on and using such devices. This policy applies to all GP Strategies incorporated entities and brands (collectively referred to hereinafter as, "**GP Strategies**" or the "**Company**") and communications concerning the Company's affiliates and parent companies (collectively referred to hereinafter as, "**Affiliates**"). Employees who violate this policy will be subject to disciplinary action, up to and including suspension or termination of employment.

3. Policy

3.1 Policy

It is the policy of GP Strategies to manage its internal and external Business Communications in a consistent, ethical and professional manner that facilitates the operational goals of the Company and its Affiliates within the governance structure.

3.2 Professional Conduct in the Communications Framework

GP Strategies' image and work environment depend on how its communications and records are perceived by its employees, Affiliates, parent company, customers, prospective customers, suppliers and the public. The Company's Business Communications are expected to adhere to the same professionally acceptable standards as all other business services activities, to address and include compliance issues where necessary and therefore must always adhere to Company policies governing the conduct of employees and its approved business practices.

The Company's clients increasingly entrust the Company with sensitive information (confidential and privacy) in both tangible and intangible (e.g., electronic, written and verbal) form. The Company's employees must demonstrate due vigilance during communications to protect the Company's, its Affiliates' and its clients' sensitive information.

Employees are directed to, but not limited to, these additional documents as parts of the communications framework to inform about related and supporting professional conduct to meet electronic, verbal, internal and external communications requirements: POL.XGB.002 (Business Conduct and Ethics), POL.USA.001 (Equal Employment Opportunity), POL.XGB.003 (Harassment), GP Internet Posting/Social Media Guidelines, the Data Classification and Handling Standard (STD.XGB.001), the Data Privacy and Records Management Policy (POL.XGB.018) and the Records Management Standard (STD.XGB.002).

All employees in their daily work are representatives and ambassadors of the Company. Therefore, each employee must be committed to preserving and enhancing the Company's and its Affiliates' reputation in all forms of communications.

3.3 Communications Approval Procedures in Routine, Fast Moving and a Crisis Communications Situation

It is the Company's policy to manage its Business Communications and relations with third parties, to include the media in an open and pragmatic way. Emergency situation Business Communications are no different than regular Company Business Communications except that the urgency of the situation may seem like a time to disregard the approved necessary deliberative considerations. Some fast-moving events are not necessarily emergencies, but they may be a surprise to employees, third parties and the GP Strategies trade media. Such surprises, while not centered on emergency situations, can also cause fast moving and sometimes chaotic searches for information by interested parties like stockholders, Affiliates or regulators.

In a time of fast breaking and / or emergency / crisis, employees may receive communications from many parties trying to obtain privileged information that may affect stock prices, regulatory compliance and employee privacy, health, safety and security. The Company will always try to be responsive to the legitimate interests of the media, internally with our employees, local government officials and with relevant partners. It will also be proactive in disseminating and as necessary expediting release of information about the Company,

its policies and products when it is judged to be in the best interests of the Company by corporate, executive and functional officials and / or as approved for use by the Director of Communications and senior Company officials for dissemination by local management.

During a period of perceived emerging or actual crisis or following an emergency event involving GP Strategies, its Affiliates, parent company and / or its clients, employees must avoid external verbal or written contact with third parties about events that emerge affecting our clients or Affiliates or are taking place within the Company. Such communications may start or seemingly confirm rumors that can affect Company reputation.

It is the Policy of the Company that official communications will be released by designated senior officials and / or the Communications department internally and externally to third parties. Third parties include the media and interacting on any other social medium. (See Social Media Communications guidelines) If an employee receives an external request for information or participation in a media event, prior approval must be obtained from their supervisor and the Corporate Communications department before responding / participating. As per standard process the employee is responsible for promptly notifying their supervisor of the request.

Emergency information for public consumption will be released at a corporate level or by vice presidents and above, or a designated on-location manager or subject matter manager. Important matters concerning GP Strategies (and / or its parent Company or Affiliates) internal business that are likely to be announced without prior notice or may come to public notice at a time of crisis may include:

- Emergency incidents involving our employees, Affiliates, facilities and/or those incidents involving urgent GP Strategies interactions with clients, law enforcement. regulators and local communities.
- Introduction, withdrawal, acquisition or sale of products or the acquisition or sale of businesses;
- Major personnel changes, operating procedures, organization, products or policy involving or affecting GP Strategies, its parent company and/or its Affiliates;
- Public statements, publications or media coverage relating to government actions or investigations involving or affecting GP Strategies and / or its Affiliates; and
- Litigation issues involving or affecting GP Strategies, parent Company and / or its Affiliates.

3.4 Business Purpose Use for Electronic Communication Media

The software and equipment and the internal and external technology services utilized by the Company and its employees in the course of their employment are intended solely to advance the business interests of the Company. Personal use by employees is generally not compatible with advancing the Company's interests and may lead to disciplinary action, up to and including termination of employment. Electronic communication media made available to employees by the Company may not be used for advocating political, religious or other personal opinions or causes that have not been specifically pre-approved in each instance, in writing, by the CEO.

Electronic communication media may not be used by an employee for personal benefit or recreation, except as otherwise authorized under this policy. All such media utilized by the Company are intended for use as business tools only. Employees should not seek access to sensitive information relating to the Company, its employees, Affiliates or clients that is not necessary for them to perform their assigned duties. Employees who violate this policy will be subject to disciplinary action, up to and including suspension or termination of employment.

Business Communications, as property of the Company, are not allowed to be transferred to personal electronic equipment for other use not compatible with the Company use or for personal use that has been restricted by contract or by a Non-Disclosure Agreement (NDA) agreed to by the Company or where prohibited by law or by the Company. Any information transfers to personal equipment must also align with the bring your own device policies and practices.

Exception: An exception to this policy is granted for personal or family emergencies. Employees may receive and / or respond to an initial message(s) concerning a personal or family emergency using the Company's electronic equipment. All such emergency communications must remain in compliance with information technology security and sensitive data handling Policies, Standards and Standard Operating Procedures. It is the position of the Company that routine personal, non-emergency, communications reduce employee attention to assigned work, and therefore, must be limited and infrequent.

3.5 Business Communications Monitoring

The Company reserves the right, and informs employees in various periodic methods that it monitors Business Communications periodically or more frequently for cause, within the framework of applicable laws, to:

(i) determine which employees will have access to data and electronic communications media,
(ii) place such restrictions or limits on the use of such media or data as the Company shall deem to be necessary or appropriate in its discretion,
(iii) monitor for noncompliance with, or circumvention of the existing restrictions or limits,
(iv) refuse or deny access to or use of electronic media or system connections,
(v) monitor usage of electronic media by employees, including all communications by way of such media,
(vi) monitor computers and other devices for compliance with current software licensing contracts and laws,
(vii) protect employee safety and security,
(viii) protect employee and company data, and
(ix) take such disciplinary action, up to and including suspension or termination of employment, as the Company deems to be appropriate in response to instances and outcomes of the above to include of unauthorized access, disclosure, use, misuse, data software and systems contamination, recklessness or other use of electronic media or data by employees which violates Company Policies or Procedures, government regulations or which the Company determines in its discretion to not be in the best interests of the Company.

Employees desiring privacy for any personal communications should not utilize Company communications media for such purposes.

3.6 Employee Protection of Sensitive Information

GP Strategies technology affords tremendous opportunities for rapidly transmitting, receiving and storing information in support of Business Communications. Employees must at all times protect against unauthorized information transmission or disclosure of the Company's and its Affiliates', vendors', sub-contractors' and clients' intellectual property and confidential information (including but not limited to copyrighted materials, employee personal privacy information, financial data, trends and projections, and other data which could adversely affect the Company's competitive position and business prospects).

Employees must guard against receiving or using unauthorized Business Communications and / or defective intellectual property received from within and outside the Company, including unauthorized copies of copyrighted software and computer code containing "contaminants". It is illegal to copy copyrighted software without permission of the copyright owner, subscribe to software not authorized by the Company and the Company prohibits the use of unlicensed, "pirated", personal or otherwise unauthorized software on Company computers. Any questions regarding the legitimacy of software found on a Company computer or acquisition and installation of new (non-standard) software should be addressed to the Corporate IT department for vetting. The Company will acquire sufficient authorized copies (subscriptions) of software necessary to conduct its business.

4. Definitions

Applicable Laws – includes the General Data Protection Regulation (GDPR) of the European Union and the United Kingdom, which is the GP Strategies, approved by the Company Privacy Policy, administrative threshold for privacy data handling; laws of any country similar to the GDPR; Section 5 of the Federal Trade Commission Act prohibiting unfair and deceptive acts in or affecting commerce (15 U.S.C. § 45(a)); and the False Statements Act (18 U.S.C. § 1001).

Contaminants – means any data, information, image, program, signal or sound that is designed or has the capability to (a) contaminate, corrupt, consume, damage, destroy, disrupt, modify, record or transmit; or (b) cause to be contaminated, corrupted, consumed, damaged, destroyed, disrupted, modified, recorded or transmitted, any other data, information, image, program, signal or sound contained in a computer or similar device, system or network without the knowledge or consent of the person who owns the other data, information, image, program, signal or sound or the computer, device, system or network. The term includes, without limitation (a) a virus, worm, or Trojan horse; (b) spyware that tracks computer activity and is capable of recording and transmitting such information to third parties; or (c) any other similar data, information, image, program, signal, or sound that is designed or has the capability to prevent, impede, delay, or disrupt the normal operation or use of any component, device, equipment, system, or network.

Sensitive Data or Sensitive Information – these terms include Company, client and client customer data that is (any of) government classified, employee-facility-planning data, safety-security-technology related data, regulated privacy data and / or contract covered confidential data.

5. References (Related Documentation)

POL.XGB.002 (Business Conduct and Ethics)

POL.USA.001 (Equal Employment Opportunity)

POL.XGB.003 (Harassment)

GP Internet Posting/Social Media Guidelines

STD.XGB.001 (GP Information Classification and Information Handling Standard)

POL.XGB.018 (Data Privacy and Records Management Policy)

STD.XGB.002 (Records Management Standard)

6. Administration of This Policy

The Company expressly reserves the right to change, modify, or delete the provisions of this Policy and any others without notice. The Company Governance Committee inclusive as needed for the review with, GP Strategies' Communications & Marketing Department / Legal Department / IT Department / Risk-Audit-Compliance-Security (RACS), is responsible for the administration and review of this Policy and will update it as needed and at least annually. All employees are responsible for consulting and complying with the most current version of this Policy. For questions regarding this Policy that are not addressed in this Policy, please contact the Company's Communications Department / Legal Department / IT Department / RACS.

7. Document Change Control

Date	Version	Reason for Change	Author
NOV 29, 2012	1.0	Initiation	Young, Matt
NOV 29, 2013	1.0	Approval	Young, Matt
NOV 29, 2014	1.0	Approval	Young, Matt
NOV 29, 2015	1.0	Approval	Young, Matt
NOV 29, 2016	1.0	Approval	Young, Matt
NOV 29, 2017	1.0	Approval	Young, Matt
NOV 22, 2018	2.0	New format	Fobes, Timothy
NOV 29, 2018	2.0	Approval	Young, Matt
NOV 20, 2019	3.0	Crisis Mgmt. language added	LaFleur, Joe
NOV 29, 2019	3.0	Approval	Matt Young, Jim Galante, Nancy Williams
NOV 29, 2020	3.0	Approval	Young, Matt/Galante, Jim/ Williams, Nancy
JAN 6, 2022 - March 21, 2022	4.0	Review/updated language/clarified-moved scope to purpose/updated links/New owner in Legal/ added 2 references/new 3.1 and expanded 3.3. Ownership changed to N. Williams	IT Documentation Team, Johnson Paula, Nancy Williams, Joe LaFleur, Company Governance Committee, Adam Stedham

END

###