Global Policy on Acceptable Use of Information Technology

Version 0.0 | June 2024

Gallagher

Insurance | Risk Management | Consulting

Policy Creation

This Policy is designed to establish rules and guidelines for the Acceptable Use and Prohibited Use of Technology.

Document Management	
Version:	0
Document ID:	GPO_AUP_00
Date:	June 2024
Review Date:	June 2025
Authors:	Global Chief Privacy Officer Chief Information Security Officer
Business Owner	Global Chief Privacy Officer
Approval	Chief Information Security Officer

Version	Date	Author	Amendments
0.0	April 2024	GCIS and Global Privacy Office	Initial Version

1. Introduction

1.1 Our Employees, clients and regulators expect and require that we protect their information. Meeting these expectations and requirements is key to our ongoing success and requires the responsible use of Information Technology. Arthur J. Gallagher & Company and its subsidiaries and affiliates (the "**Company**", "**Gallagher**", "**we**", "**us**", "**our**") are committed to protecting information under our care and complying with current laws and regulations. Prohibited Use of Technology exposes the Company to risks including compromise of systems and data, reputational damage, legal, regulatory, contractual, and other risks.

2. Purpose

2.1 The purpose of this Policy is to establish rules and guidelines for the Acceptable Use and Prohibited Use of Technology.

2.2 This Policy aims to safeguard the Company, its resources, Gallagher Information, the privacy and security of Employees, clients and third parties and ensure compliance with our legal, regulatory, and contractual obligations.

3. Scope

3.1 This Policy is applicable to all officers, directors, permanent and temporary employees, Contractors, consultants, and secondees of the Company ("**you**", "**your**", "**Employee(s)**") and lays out your obligations with respect to the Acceptable Use and Prohibited Use of Technology.

3.2 This Policy must be read in conjunction with the Global Information Classification and Handling Policy, other Related Policies and any local entity policies or procedures, which may exceed but not limit the requirements within this Policy, without written approval from either the Global Chief Privacy Officer or Chief Information Security Officer.

3.3 Employees are responsible for exercising good judgement regarding both Acceptable Use and Prohibited Use of Technology in accordance with Company policies, standards, laws and regulations.

3.4 If you have questions or concerns regarding how to apply this Policy, raise these with your (1) manager, (2) your local or regional compliance lead, (3) your Business Information Security Officer, (4) your local Privacy Lead, or (5) the Global Chief Privacy Officer.

3.5 In this Policy we use the word "must" to mean a mandatory requirement. In contrast, "should" indicates that the statement is best practice, and it is recognized that there will be some circumstances in which the approach is not appropriate. You must be able to demonstrate why the approach is not appropriate if you do not adopt best practice.

4. General

4.1 The Global Privacy Office (GPO) owns this Policy and guides all Employees on the Acceptable Use and Prohibited Use of Technology.

4.2 Global Technology Services (GTS) provides guidance on the associated rules with IT.

5. Key Terms

5.1 **"Acceptable Use"** means authorized actions taken by Employees when using Technology, in compliance with this Policy, other Company policies and our legal, regulatory and contractual obligations.

5.2 **"Contractors"** means any person: 1) working on Gallagher owned, controlled, or operated sites; or 2) who is directed in their actions by a Gallagher Employee; or 3) who we have engaged to provide services to Gallagher through a recruitment agency, labour hire organisation or any other third party.

5.3 **"Gallagher Information"** means all information and records relating to the Company or the business or activities or affairs of the Company, including but not limited to financial records, strategic plans, internal business policies, customer lists, prospect lists, pricing information and any information about our clients, prospects, markets, Employees and suppliers (including information they share with us).

5.4 "**Handling**", "**Handle**" or "**Handled**" means creating, collecting, storing, moving, sharing, or destroying Gallagher Information.

5.5 **"Personal Device"** means any device used by an Employee to Handle Gallagher Information other than Gallagher provided computer equipment.

5.6 "**Prohibited Material**" includes, but is not limited to:

- Material which is pornographic or obscene, or which contains or advocates any form of violence, abuse, exploitation, defamation, harassment, bullying, intimidation, or other objectionable activities;
- Material which contains or advocates any form of discrimination based on any protected characteristic. Examples include race, national identity, family responsibilities, marital status, physical features, sex, sexual orientation, gender identity, lawful sexual activity, (potential)pregnancy, disability, age, health status or medical record, breastfeeding, political or religious belief, employee association membership, criminal record where not relevant to professional requirements);
- False or misleading material (which may include using an anonymous or misleading identity);
- Gambling material (except as approved at Company-sponsored events);
- Material which may infringe intellectual property rights (including software applications and copyrighted text), or which may not be copied without proper authorization; and
- Any material prohibited by law in the jurisdiction where the material is handled.

5.7 **"Prohibited Use"** means unauthorized actions taken by Employees when they use Technology, in contravention of this Policy, other Company policies or our legal, regulatory, and contractual obligations.

5.8 **"Technology"** means any Gallagher approved applications or messaging systems, Gallagher provided computer equipment and, when used to Handle Gallagher Information, Personal Devices.

5.9 **"Third-party Messaging Platform"** means a technology platform or application, neither owned nor provided by Gallagher, that enables individuals to communicate with others. This includes, but is not limited to:

- Mobile messaging platforms (e.g., text messaging, SMS, iMessage, Google Messages);
- Ephemeral messaging platforms (e.g., WhatsApp, Signal, Snapchat, Telegram), designed to have messages disappear or otherwise be deleted a period of time after sending/posting;
- Social media messaging (e.g., Facebook Messenger, Twitter); and
- Other online message services or platforms (e.g., email, forum user messages).

6. Policy Statements

6.1 Gallagher Information stored or processed on Devices, remains the sole property of Gallagher. Employees must protect and lawfully use Gallagher Information in accordance with our:

- Global Business Conduct Standards;
- Global Information Privacy Policy; and
- Global Information Classification and Handling Policy.

6.2 When you use Technology, you must follow the Acceptable Use and Prohibited Use rules below:

Topic	Acceptable Use – You MUST:	Prohibited Use – You MUST NOT:
General	• Use Technology in a manner that protects the privacy and security of Gallagher Information, the Gallagher brand/ reputation and complies with our legal, regulatory, and contractual obligations. • Use Gallagher provided computer equipment, approved applications and messaging systems for legitimate business purposes, with only incidental, minimal personal use allowed, such as accessing news services during legitimate work breaks or contacting family members while on business travel. • Report any inappropriate communication received via the Company's Technology to your manager and/or Corporate Human Resources.	• Use Gallagher provided computer equipment, approved applications or messaging systems, including when on a Personal Device, to conduct business activities not related to Gallagher. • Use Technology in contravention of laws including those relating to privacy, spam, unsolicited emails, misleading/deceptive conduct, copyright, libel, defamation, health and safety, employment practices, equal opportunity, discrimination, harassment, criminal conduct, and bullying. • Use the Company's systems to solicit for personal, social, charitable, commercial, religious or political causes or ventures, without approval from a Divisional or more senior leader.
Security	• Secure Technology with an automatic locking screensaver set to 10 minutes or less. • Lock or log off from Technology when no longer actively using it and clear desks of hard copy Gallagher Information when not at your work station. • Safeguard passwords and access account information to Technology. Employees are responsible for their use of and access to Technology, and accounts established in their name. • Keep Technology secure and protected from accidental loss or damage. Notify your manager and IT immediately if any Gallagher provided computer equipment is lost or damaged or a Personal Device is lost.	• Attempt to bypass any installed security protocols (these include Gallagher controls to assist with the blocking of unapproved Internet sites and access control measures) on Technology. This could have significant adverse impacts to the security of Technology or Gallagher Information. • Intercept data of which you are not the intended recipient. • Log into a server or account without appropriate authorization. • Share passwords to Technology, including with any member of IT. • Access Technology using someone else's username and password.

Topic	Acceptable Use – You MUST:	Prohibited Use – You MUST NOT:
Prohibited Material and Malware	• In the event you inadvertently receive or view Prohibited Material on any Technology, advise your manager and the Legal team, and follow their instructions.	• Use Technology to create, download, store, copy, distribute (or knowingly receive) Prohibited Material or files infected with malware.
Electronic Communications including Email	• Send electronic communications that meet standards acceptable for ordinary business correspondence. • Comply with the Handling rules for Gallagher Information as detailed in the Global Information Classification and Handling Policy.	• Send electronic communications which may harm the Gallagher brand or business. • Send Gallagher Information to your personal email account or any unauthorized recipient without approval from the Legal Team. This does not prevent you sending your personal pay slips or other of your HR-related data to your personal email. • Upload/send file attachments from your personal email account when accessed from Gallagher provided computer equipment. • Auto-forward messages from your Gallagher email account to a non-Gallagher email account. • Auto forward messages from a non-Gallagher email account to your Gallagher email account. • Send unsolicited electronic communications containing advertising or promoting goods, services, business, or investment opportunities without permission from the Marketing Department. • Contravene the Handling rules for Gallagher Information as detailed in the Global Information Classification and Handling Policy.
Social Media, Gallagher Brands and Copyright	• Ensure you comply with the Social Media Policy when using Technology.	• Use your Gallagher account or password for the creation of social media accounts without approval from the Marketing Department. • Use a Gallagher brand or copyright material (e.g. Company logos, trademarks, or images) without approval from your manager or the Legal Team.

Topic	Acceptable Use – You MUST:	Prohibited Use – You MUST NOT:
Software and Systems	• Use Technology in accordance with relevant licensing agreements, Company policies, laws, and regulations.	• Download or install software onto Gallagher provided computer equipment without approval from IT. • Enter into agreements with external IT service providers (e.g. external business applications, hosting, web services, exchange of Gallagher data) without approval from IT Management. • Upload or transmit software or any copyrighted materials belonging to Gallagher or any third party without approval from the owner of the software or material. • Intentionally interfere with the normal operation of Technology e.g., disabling security controls, connecting Gallagher provided computer equipment to systems not used to support Gallagher business, or propagating malware.
Personal Devices	• Exercise care in tethering your Gallagher Technology to any non-Gallagher Device (hot-spotting) where necessary to support Gallagher business. • Only connect the following external devices to Gallagher computer equipment: webcams, speakers, headphones, keyboards, mice, docking stations, monitors, personal printers where authorized, and wired or wireless network devices necessary to connect to the public Internet and the Gallagher network. • Only use Gallagher approved applications and messaging systems to Handle Gallagher Information.	• Connect Personal Devices to Gallagher computer equipment (including our network) whether by physical cable, Bluetooth or WiFi (other than as expressly permitted by this Policy). • Use Gallagher approved messaging systems and applications for activities not related to the business of Gallagher. • Use Third Party Messaging Platforms to Handle Gallagher Information.

Working Remotely From Another Country	• Remove Intune (which provides access to Gallagher email, Microsoft Teams and other Gallagher Information) from any personal device(s) before taking such device(s) to any of the prohibited locations.
	• If you have inadvertently or temporarily stored any files to your laptop's local storage (hard drive, desktop), copy
		• Take Gallagher Technology to the following locations:
		  • Belarus
		  • Cuba
		  • Iran
		  • North Korea
		  • Russia
		  • Syria

Topic	Acceptable Use – You MUST:	Prohibited Use – You MUST NOT:
	these files to your OneDrive and remove the local copies prior to travelling. • In the event that you are required to divulge Gallagher credentials or turn over any Technology, report the incident to Cyber_Security@ajg.com immediately and, as soon as permitted, reset your password(s) on the device(s). • If given the current political and security landscape you believe you are travelling to a particularly high-risk country, consider not taking your Gallagher device(s), removing Intune from any device(s) you plan to take with you and/or avoid working remotely from that country. Seek guidance from your Business Information Security Officer if you are unsure. • Avoid using public Wi-Fi networks, such as those found in cafes or airports, as they are often unsecured. If remote working is necessary from those locations, use a known entity-owned hotspot, or your own wireless phone provider's hotspot functionality when connecting from untrusted locations. If your device's battery is low, use either your own battery pack or your own charger plugged into a power outlet to charge. Public charging outlets with USB connectors can be used to spread malware. Avoid entering user IDs and passwords on any publicly available computer (library, kiosk, etc.).	• Venezuela • Hand over any Gallagher device or personal device if either logged into Gallagher resources or which contains Intune, or any passwords to such devices to anyone unless you are legally required to. • Not connect or pair your device with any rental car's entertainment or navigation systems.

7. Notice of Monitoring

7.1 Subject to applicable law, in order to protect Gallagher Information, our legitimate business interests and ensure compliance with Company policies, standards, procedures and our legal, regulatory, contractual and confidentiality obligations, the Company may monitor (using both manual and automated methods) your use of Technology including any Handling of Gallagher Information on Third-Party Messaging Systems.

7.2 Subject to applicable law, Employees have no expectation of privacy when using Technology. By accessing or using Technology, including when using Gallagher approved applications and messaging systems on a Personal Device, Employees acknowledge that the Company may monitor their use. Employees must not use Gallagher provided computer equipment or Gallagher approved applications or messaging systems for personal use if they do not wish their personal use and communications to be monitored.

7.3 Subject to applicable law, if Gallagher has a reasonable suspicion of your noncompliance with this Policy, any other Company Policy, our legal, regulatory or contractual obligations, or at the request of a regulator to provide evidence of communications or business records, the Company may request access to inspect and conduct a reasonable search of your Personal Device. Your failure to cooperate in these circumstances may result in disciplinary action, up to and including termination of your employment or engagement with the Company.

7.4 Monitoring activities, logs and results may be accessed by management, Information Technology, Security, Human Resources, Compliance, Privacy, Legal, Internal Audit, external advisors and experts authorized and acting on behalf of Gallagher as well as regulatory bodies and law enforcement authorities. This may include any person auditing compliance with the Company's policies, standards, procedures, and our legal, regulatory, and contractual obligations as well as those undertaking forensic examinations.

7.5 Monitoring activities may result in disciplinary action and/or legal proceedings.

8. Training

8.1 Employees must be trained so that they understand their obligations under this Policy.

9. Employee Acknowledgement

9.1 Use of Technology constitutes an Employee's acceptance of this Policy and agreement to abide by its terms.

10. Non-Compliance with This Policy

10.1 Non-compliance with this Policy may result in disciplinary action by Gallagher, up to and including termination of your employment.

10.2 The Company may advise law enforcement officials of any employee violations of the law.

10.3 Where there is a justifiable business case for non-compliance with this Policy, a written waiver can be requested from either the Global Chief Privacy Officer or Chief Information Security Officer.

11. Related Documents

11.1 Related policies:

Global Business Conduct Standards
Global Information Privacy Policy
Global Information Classification and Handling Policy