Document ID: GPO_ICH_02	**Title: Global Information Classification and Handling Policy**
Effective Date: 1 June 2024	**Revision No. 2**
Business Process Owner:	**Global Chief Privacy Officer and Chief Information Security Officer**
Document Type: Policy and Governance	**Exhibits: N/A**

Overview & Purpose

Our employees, clients and regulators expect and require that we protect their information. Meeting these expectations and requirements is key to our ongoing success. 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.

The purpose of this Policy is to ensure the appropriate Classification and Handling of Gallagher Information.

Scope

This Policy is applicable to all officers, directors, permanent and temporary employees, contractors, consultants, and secondees of the Company ("**you**", "**your**", "**Employees**") and lays out their obligations with respect to Classification and Handling of Gallagher Information.

This Policy must be read in conjunction with local entity procedures, which may set more stringent requirements but which may not lower the requirements within this Policy, without the written authorization from either the Global Chief Privacy Officer or Chief Information Security Officer.

The Gallagher Information Classification Schema and Handling Rules contained within this Policy apply to all Gallagher Information irrespective of when it was created.

If you have questions or concerns regarding how to apply this Policy, you can raise these with your (1) manager, (2) local or regional compliance, (3) your BISO, or (4) data privacy personnel.

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 recognised 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.

Policy

1.0 Definitions

"**Artificial Intelligence System/AI System**" means any Gallagher, third-party or publicly accessible system or application that is designed to operate with elements of autonomy to produce system-generated outputs such as content, predictions and decisions, and infers how to achieve a given set of objectives based on data and inputs and which does so using machine learning and knowledge-based approaches. Examples of AI systems include ChatGPT, Bard (Chatbot) and DALL-E (image/media creation tool), chatbots, summarization and translation tools as well as in-house insurance pricing algorithms that update prices in real time based on learnings the system makes from insurance claims.

"Classify/Classified/Classification" means the process by which Employees assess Gallagher Information they create, receive, hold or share and apply the correct classification level (Public, Confidential or Restricted) based upon the criteria within Gallagher's Information Classification Schema. The classification level drives how Employees Handle the Gallagher Information.

"Compromise" means the loss, corruption, misuse or unauthorized disclosure of Gallagher Information.

"Handling/Handle" means creating, collecting, storing, moving, sharing or destroying Gallagher Information.

"Gallagher Approved Application/Messaging System" means software and platforms (such as Gallagher email or Gallagher Microsoft Teams) provided by or made available by the Company for installation on Company or personal devices for transacting Gallagher business, communicating with Employees, clients and/or business contacts and/or transmitting Gallagher Information to authorized recipients.

"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).

"Information Classification Schema" means the schema you must use to determine the classification of the relevant Gallagher Information for the purposes of determining and applying Handling rules.

"Record" means any record of Gallagher Information, regardless of its form, that is created or received by any Gallagher Employee. Records may be in electronic or hard-copy form, including but not limited to paper documents, electronic files (whether on hard drives or other storage media), internal or external correspondence, publications, books, pictures, videos, audio recordings, maps, drawings, and other forms of information.

"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).

2.0 Information Classification Schema

Gallagher Information must be Classified into one of three categories (or one from a Government classification scheme if required locally) in order that you know what Handling rules to apply when you store and, where necessary, share it. Our three Classification categories are:

- Public
- Confidential
- Restricted

The Classification level is dependent upon the potential impact and harm if the information is Compromised.

A Record that contains multiple Classification categories must be Classified according to the highest level of Classification category e.g. if a Record contains ‘**Confidential’** as well as ‘**Restricted’** data, you must Classify and Handle the entire Record as ‘**Restricted’**.

Information Classification Schema

See the table below for the definitions of Gallagher's three Classification categories and high-level examples of what information falls into each category.

Classification	Public	Confidential	Restricted
Definition:	Gallagher Information, if accessed, disclosed, altered or destroyed, without authority, could result in the following level of financial, regulatory or reputational impact to Gallagher or its clients /markets:		
	None	**Up to a high level**	**Up to a very high level**
Characteristics:	Records Gallagher has formally approved may be made available to the public at large. There are no restrictions on who these can be shared with	All Records, unless they fall into the **Public** or **Restricted** Classifications	All Records that contain any one or more of: • Sensitive personal information or special category data e.g. racial or ethnic origin, religious beliefs, trade union membership, medical or health conditions, sexual orientation or identity, gender identity, criminal offences and/or proceedings and national identifiers • Individuals' salary, remuneration, compensation data, bank details, credit/debit card information (numbers, PINs, CVV, etc.), tax information, life insurance, financial information obtained as a result of credit, pension and/or benefits information, all in combination with information that identifies an individual • Gallagher Information that, if released, is likely to cause harm to an individual e.g. home addresses of those with kidnap and ransom insurance etc. • Mergers and acquisitions information • Cyber insurance coverage and claims • Information a Gallagher client/market has specified must be handled as '**Restricted'** • Information on the management of Gallagher or our client's businesses that if released, either internally or externally, to unauthorized individuals could cause significant harm to the business or its share price such as: ◦ Board, Audit, Executive and Risk Committee papers ◦ Budget data, unapproved and/or unpublished accounts, bank records ◦ Business strategies ◦ Client lists ◦ Product pricing, algorithms, data models or actuarial calculations ◦ Source code / analytics algorithms ◦ Internal audit action findings and remediation plans

Classification	Public	Confidential	Restricted
			• Information/cyber security related data/ posture • Litigation documents • Internal / external Legal advice marked ‘privileged’ or ‘confidential’ • Market sensitive data • Risk Event data (including related to data incidents or breaches) • HR, Compliance or other Company investigation data • Property drawings and maps • IT Network diagrams, passwords, encryption keys or security vulnerabilities-related data • Anything restricted by law/regulation; e.g. International Traffic In Arms Regulations (ITAR) / Export Administration Regulations (EAR)

3.0 Handling Rules – All Employees

It is your responsibility to determine the Classification of your Record. Once you have, use the tables on the following pages to determine how to store and share it securely with authorized recipients.

Any request to deviate below the minimum Handling requirements must be made to and approved in writing by either our Global Chief Privacy Officer or Chief Information Security Officer, who will hold a register of approved exceptions.

By default, Handle all Gallagher Information in accordance with the rules for ‘**Confidential’** information. It is your responsibility to ensure you are clear on what qualifies as ‘**Restricted’** Gallagher Information and apply those specific Handling rules accordingly. Do not guess if a Record is ‘**Public’**. It is your responsibility to know whether a Record is classified as ‘**Public’** before you Handle it accordingly.

Some AI Systems, such as ChatGPT, Bard and DALL-E are made available to the public, and others, such as Microsoft 365 Copilot and Grammarly, are offered for sale or licensing by their developers. Information entered into these tools, as well as information they intake autonomously to learn, becomes part of the AI System’s learning data sets. Users, and in some cases the developers themselves, can no longer control how this information is stored and shared. To help us ensure we comply with our contractual and legal obligations you must follow all Handling Rules. Please note that the Company has visibility to all uploads of data from the Gallagher network to AI Systems, and reserves the right to take disciplinary action, up to and including termination, in the event of non-compliance with these Handling rules.

Handling Rules for Gallagher Information– All Employees

Activity	Public	Confidential	Restricted
General Handling Rules	• No restriction	• You must: • Only share internally / externally, on a need-to-know basis, and only with individuals who have a legitimate business need. Obtain permission from the originator where necessary • Validate recipients are correct, are authorized to receive it and you are sharing the correct information • Promptly report actual or suspected Compromise of Gallagher Information by sending an email to Cyber_Security@ajg.com • Lock your computer screen whenever it is unattended • De-identify (remove the ability to identify what individual or client the Gallagher Information relates to) data whenever possible and separate access to identified and de-identified data sets	
			• Limit storage and collection • Mask any payment card number(s) where displayed or printed to no more than the first six and last four digits, unless the user has a legitimate business need to see the full card number
AI Systems	• No restriction if AI System is accessible from the Gallagher network. • You may use publicly accessible AI Systems to help you become more productive, but you	• You must not: • Enter any Gallagher Information classified as ‘**Confidential’** or ‘**Restricted’** into any unapproved AI System. For the avoidance of doubt, all publicly accessible AI systems are unapproved AI Systems • Input any Gallagher Information into any AI System inaccessible from the Gallagher network, and must not use such AI Systems to conduct any Gallagher business. Our network controls are implemented to prevent use of AI Systems designed for unethical or nefarious purposes • If you are using a Gallagher approved AI system, you must: • Treat output from the system as Gallagher proprietary information	

Activity	Public	Confidential	Restricted
	must abide by the rules for **Confidential** and **Restricted** data. Examples of permissible use include asking an AI System to draft a sample job description or to provide a summary of a particular topic. • All content produced by AI systems must be reviewed for accuracy and content quality by its owners prior to use.	• Handle output according to its classification level and in compliance with this and other Gallagher policies, including limitations on sharing, as applicable • Ensure that all content produced by the Gallagher approved AI system is reviewed for accuracy and content quality by its owners prior to use	
Paper: Copying / Printing / Faxing / Mailing / Storage/ Destruction	• Recycle when no longer required	• You must: • Adopt a clear desk policy when moving away from your workstation • Only print when there is a legitimate business need • If in a hotel, keep it on one's person or lock it out of sight in the hotel room • If left in a car, lock it away and out of sight • If working from home, lock it in a cabinet / drawer or in a locked room when not in active use and lock your home when unattended • Use a data-encrypted fax service for fax transmissions and the recipient must be waiting at the receiving fax	

Activity	Public	Confidential	Restricted
		• Subject to Gallagher's Record and Information Management Policy and retention periods, deposit paper into a Gallagher secure shredder / shredding bin when no longer required or shred at home using a cross cut shredder • Only scan Records to a Gallagher email address. If you need to forward scanned documents to third parties, do so using your Gallagher email account and not directly from a scanner • For internal / external post, use a sealed envelope with only sender and recipient name and address visible • Must not be left unattended: • On a printer/fax • In unrestricted Gallagher office areas e.g., areas open to visitors such as reception / meeting rooms • If travelling or on a customer site	
		• You must: • Within a Gallagher office, lock it in a cabinet / drawer during out of office hours	• You must: • Within a Gallagher office, lock it in a cabinet / drawer when not in active use • You should: • External Post: use a sealed tamperproof package, tracking services and delivery confirmation • Internal Post (i.e. Internal Office Mail): hand deliver by Gallagher member of staff or courier when being transferred between Gallagher offices

Activity	Public	Confidential	Restricted
Email from a Gallagher Email Account to Another Gallagher Email Account	• You must: • Use a Gallagher approved email account for conducting Gallagher business and sharing Gallagher Information • State the name of the sender if you are using a Gallagher group mailbox • Before forwarding on an email, consider checking with the sender that this is permitted • If the information is particularly sensitive or large in volume, consider password protection (to Gallagher Password Standards) and/or changing the properties of the email to 'Private' so that it cannot be read by others who may have access to the recipient's mailbox		
Email to a non-Gallagher Email Account		• You should: • Encrypt in transit using a Group approved encryption technology (Gallagher email is set to send encrypted emails in transit by default) • You must: • Send business-related emails to Employees, clients or business contacts from Gallagher Approved Application/Messaging Systems i.e. your Gallagher email account • You must not: • Send Gallagher Information to your personal email account 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	
		• You must: • Password protect attachments containing personal information (any information that can be used to identify a living individual including names, Employee ID's, addresses etc.) relating to more than 100 individuals. • The password must be a minimum of eight (8) characters	• You must: • Encrypt (using a minimum effective 128-bit key) and password protect attachments containing Restricted personal information relating to more than 10 individuals. • The password must be a minimum of eight (8) characters in length, be complex and contain a combination of uppercase and lowercase letters with numbers or special characters.

Activity	Public	Confidential	Restricted
		in length, be complex and contain a combination of uppercase and lowercase letters with numbers or special characters. - Share the password by a means other than the original email channel, such as via a telephone conversation.	- Share the password by a means other than the original email channel, such as via a telephone conversation.
Collaboration Tools e.g. Instant Messaging / desktop sharing / online meetings	- No restriction	- You must: - Use Gallagher Approved Application/Messaging Systems to conduct business communications and transmit Gallagher Information, such as Gallagher Microsoft Teams. - Ensure recipients are known to you and are either Gallagher Employees or third parties who are subject to a confidentiality agreement such as clients, business contacts or suppliers - Be careful of the language you use and the Gallagher Information you share including Microsoft Teams chat - Ensure we have auditable Records of all business conducted with Employees, clients and business contacts and they are stored on Company devices. - You must not: - Share Gallagher Information via a Third-party Messaging Platform - Use assistive functionality that transfers Gallagher Information to third parties (e.g., Siri, Google Translate)	
Third-Party Messaging Platform	- You must: - Use Gallagher Approved Application/Messaging Systems to conduct business communications and transmit Gallagher Information. - If you use a personal device, only Gallagher Approved Application/Messaging Systems may be used on that personal device for electronic communications related to your Gallagher employment responsibilities/Gallagher business activities, particularly (but not exclusively) when creating, storing, or processing Gallagher Information.		

Activity	Public	Confidential	Restricted
	• You must not: • Use any Third-Party Messaging Platform to conduct business communications or transmit Gallagher Information.		
Client Approved Online Portal	• You must: • Only use portals that meet Gallagher’s Group encryption in transit and at rest requirements, that have been approved for use by local information security and reviewed in line with our Access Management Policy		
Unapproved Online Portal / Cloud Storage	• You must not: • Upload Gallagher Information to personal cloud storage or any portal / cloud storage solutions not approved by Gallagher Technology Services (GTS)		
Portable Storage e.g. USB devices, SD card, DVD, hard drive	• You must not: • Use a portable storage device to store the master copy of a Gallagher Record • Plug a storage device into any Company device until approved by local IT • You must: • Contact local IT Staff and follow approved process if you receive a USB thumb drive, SD card, CD/DVD or hard drive from a third party • Only use storage devices in limited circumstances, such as a backup of an internal presentation for an internal conference or to share large files with a client or business contact • Encrypt Records saved to the storage device • Ensure the recipient is authorised to receive the Records • Delete the Gallagher Information immediately when it is no longer required		
		• You must: • Obtain approval from your Manager and Privacy Lead to download to a storage device if you need to share files externally	

Activity	Public	Confidential	Restricted
		• Only use a storage device in limited circumstances to transfer Gallagher Information such as the provision of multiple client files that are too large to be sent by email or stored to small capacity externally encrypted media.	

4.0 Training

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

5.0 Implementation

Each division of the Company shall be individually responsible for assuring that the branches, offices, departments, or other business units within that division implement and comply with this Policy. Implementation of this Policy shall include:

- Each Chief Operating Officer (or equivalent) should designate an individual with responsibility for implementing and facilitating compliance with this Policy; and

- If the Company creates a new division, organization, branch, or other business unit, then that new division, organization, branch, or other business unit is responsible for implementing this Policy immediately. However, if the Company acquires or merges with an existing company, any acquired/merged division, organization, branch, or other business unit shall implement this Policy and any relevant Appendices within one (1) year of the merger/acquisition.

6.0 Non-Compliance with This Policy

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

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

7.0 Related Documents

Related policies

Global Record and Information Management Policy.
Global IT Policy Manual