Effective Date:	October 2016
Distribution:	All Realogy Employees
Policy Owner:	Ethics & Compliance Department
Version:	2

The Information Management Policy

Table of Contents

1.0	**Introduction and Summary**	**1**
2.0	**Information Creation, Management and Disposal**	**3**
3.0	**Protected Information**	**7**
4.0	**Privileged Information**	**11**
5.0	**Hold Management**	**12**
6.0	**Storage and Disposal of Paper Information**	**14**
7.0	**Vital Records**	**15**
8.0	**Roles and Responsibilities**	**15**
9.0	**Policy Compliance Audits**	**18**
10.0	**Risk Policy Requirements**	**18**

1.0 Introduction and Summary

At Realogy, we understand how important Information is – and how important it is that we manage our Information properly for the benefit of our company (Realogy, its Business Units and subsidiaries), business partners and customers. We take seriously our responsibility to manage our Information (as defined below) according to our internal policies and the law.

Our Information Management Policy **("Policy"**), including the Realogy Record Retention Schedule (which is incorporated into this Policy), is intended to guide employees and non-employees who handle our Information to ensure the consistent, organized, and secure management of our company's Information. We want to manage our Information so that:

- We have the Information we need,
- We can access Information in an efficient and organized way when we need it, and
- We are protecting Information as required by law and our business policies, including timely Disposal of Information we are no longer required to keep.

1.1 What is Information?

For purposes of this Policy, Information is both digital and physical; it includes a wide variety of documents and data that you may handle or have access to as part of your work for Realogy. We define **"Information"** broadly as data in any form (printed or digital) created by, managed by, owned or licensed by, or in the custody of Realogy. Information will include, without limitation, messages, notes, memos, customer/client/vendor lists, customer/client/vendor information, presentations, marketing materials, vendor lists, drafts, financial information, contracts, correspondence, third-party licensed material, video, photographs and recordings.

All capitalized terms of this Policy will be defined in the Appendix.

1.2 What is Information Management?

Information management is our process for creating, storing, organizing, protecting, securing and destroying Information. It involves Realogy policies and procedures that allow our employees and non-employees to understand how to treat Information.

1.3 Why Do We Need Information Management?

As the volume of Information we handle grows every day, we need to develop and utilize more consistent and sophisticated ways to organize, sort, track, retrieve, protect and dispose of it – all in accordance with our company's policies and the law. We need to make sure we (a) have easy access to the Information we need to operate, (b) retain Information subject to a legal preservation notice or Hold (as defined in Section 5) or regulatory record-keeping requirements, (c) protect Information we need to retain, and (d) dispose of Information that we are no longer required to keep to improve efficiency, reduce retention and storage costs, and help ensure it does not fall into the wrong hands.

This last requirement is an important consideration. As a person handling Realogy Information, you may find it easier to retain every document, every email and every draft to guarantee that you have a complete history. But that practice is not compliant with this Policy (and in some jurisdictions, it may not be compliant with applicable law). The practice of saving all Information increases our costs in retaining and storing Information, adds to our expenses in responding to requests for Information in litigation or other regulatory proceedings, and maintains personal or confidential Information for a longer period of time than necessary (which increases the risk that the Information may be compromised). Information Management requires that we take care of our Information in a more thoughtful way. It demands that we identify which Information must be kept and which must be discarded for our company's benefit and for the benefit of our customers, clients, vendors and partners who entrust their Information to us.

1.4 Who Does This Policy Apply To?

This Policy applies to all personnel of Realogy and its subsidiaries, including employees, temporary staff, outsourced partners, service providers, and any other person or entity who has been granted access to Information or to Realogy Information Technology Resources. **"Realogy Information Technology Resources"** refers, but is not limited, to networks and servers, email and website platforms, desktop PCs, laptops, tablets, mobile phones, smart phones, printing devices, telephones, facsimile machines, Realogy-controlled social media platforms, databases, voicemail systems and any other electronic device capable of storing or transmitting information, including e-mail, instant messaging and Internet access provided by Realogy. The software installed on such devices and resources is also included. Realogy Information Technology Resources may also refer to non-Realogy host or server computers, stand-alone computers, laptops and any other communication devices, software, data files and networks when used to perform Realogy business.

Unless applicable law or agreement states otherwise, if you violate this Policy, you may be subject to disciplinary action, and you and Realogy may face potential civil and criminal liability.

1.5 Conflicts

If this Policy conflicts with any applicable law, we will follow the applicable law; however, please notify Realogy's Ethics & Compliance department at ethics.compliance@realogy.com if you discover any actual or potential conflict between this Policy and the law. Subject to applicable laws, this Policy is not intended to change or limit Realogy's legal or contractual obligations to return, destroy or otherwise not retain Confidential, Highly Confidential or Restricted Confidential Information.

1.6 Policy Updates

This Policy is maintained at http://athome.realogy.com, along with the Record Retention Schedule, which is made a part of this Policy. Updates to the Policy or the Record Retention Schedule will be available on the Realogy AtHome intranet site. If you have any questions about this Policy, contact your manager, a member of the Legal department, or an Ethics & Compliance Officer.

2.0 Information Creation, Management and Disposal

Every day, most of us create business records as a normal part of performing our jobs. We send and receive emails; we generate contracts, drafts, marketing materials, financial analyses, customer lists and memos. We make progress against our business goals, which typically means that we create Information along the way. As we create Information, we need to give some thought to how it will be managed. Information should be managed on a daily basis, including organizing, storing and disposing of Information under the guidelines of this Policy.

2.1 Types of Information

Our Information is an asset belonging to Realogy. It is critical to Realogy's success that we manage these assets responsibly. Managing Information appropriately under this Policy requires that you understand the types of Information created at our company and how to treat those types of Information. At Realogy, we recognize two types of Information: (1) Works in Progress; and (2) Final Business Records. Within your office, cubicle or computer, you may also have Non-Records, which are not considered Information for purposes of this Policy.

2.1.1 A **"Work in Progress"** is Information created for a particular project or assignment that must be retained for the duration of the project or assignment on Realogy's behalf. If any Information is needed for ongoing work – even if the work extends for several months or years – that Information is considered a Work in Progress. Examples of a Work in Progress are drafts, project plans, notes, work papers, support documents, working files, related emails, and informal correspondence related to work/project activities. A Work in Progress will usually culminate in a Final Business Record with the successful completion of a project or assignment, or if the project does not come to fruition, a Work in Progress may become the Final Business Record for purposes of this Policy.

2.1.2 A **"Final Business Record"** is Information that represents a final project deliverable or it could be a document or digital file – correspondence, email or other documents – that records our business activities in the ordinary course. Final Business Records must be retained for legal and business reasons for a defined period of time under the Record Retention Schedule. Examples of Final Business Records are executed contracts, correspondence, business email (including final email chains that document all discussion threads), memos, performance appraisals, audit reports, year-end financials, balance sheets, marketing campaigns and Realogy training materials.

2.1.3 A **"Non-Record"** is a document or digital file that is personal in nature, has no retention value for the company or does not involve any business transacted on behalf of the company. A Non-Record may include personal emails, calendar notes, casual messages that do not relate to Realogy business, or incidental work reference materials. Non-Records do not constitute Information under this Policy and therefore are not subject to any record retention requirements.

2.2 Record Retention Obligations

Our Record Retention Schedule is available here or at our company Intranet site https://athome.realogy.com. As its name suggests, our Record Retention Schedule details the required retention times for particular types of documents that are categorized as Final Business Records. Under applicable law and/or business policy, many of Realogy's Final Business Records must be retained for their "Active Lives" – defined as the period of time when the record is effective – plus a designated number of years.

> **EXAMPLE:** Realogy signs a U.S. information technology vendor contract with a two-year term. The Record Retention Schedule requires retention of U.S. vendor contracts for "ACT+6." Under our Policy, assuming the contract is not extended by later agreement, we must retain the vendor contract as a Final Business Record for **eight years** from the date we signed it (i.e., the contract's Active Life of two years plus an additional six-year Retention Period).

You should refer to the Record Retention Schedule regularly as you manage Information in your possession. In addition, you should consult any policies specific to your Business Unit. Realogy Business Units may designate specific processes for retaining and maintaining Information under their control. You will be responsible for complying with both this Policy and your Business Unit policies and processes.

2.2.1 Final Business Records. You are required to retain Final Business Records in your possession or under your control for the time designated in Realogy's Record Retention Schedule, unless the Information is subject to a longer Retention Period under a Hold (discussed in Section 5 below). When Information is duplicated in paper and electronic media, the Business Unit will determine, in consultation with their legal advisors (including the legal team handling litigation for the Business Unit), whether the paper or electronic version will serve as the Final Business Record. Any changes to the designation or categories of Final Business Records to be preserved in our hard-copy and digital file systems must be approved by the Business Unit's Legal department and the Realogy Litigation department. If your Business Unit requires email and email attachments to be moved in order to be preserved, you must move any email and email attachments to Business Unit-provided repositories and retain according to the Record Retention Schedule.

2.2.2 Works in Progress. Works in Progress will be retained for the duration of the applicable project or assignment. After completion of the project or assignment, Works in Progress may be subject to Disposal, so long as the Information is not subject to a Hold (discussed in Section 5 below). You must review your electronic and printed files on a regular basis and delete or shred those files or documents no longer needed for legal or business purposes. Exact duplicate copies do not require retention as a Work in Progress so long as one copy is retained during the project duration.

2.2.3 Non-Records. You are not required to retain Non-Records. Non-Records should be moved to your personal storage or deleted or destroyed from Realogy Information Technology Resources when no longer needed.

Q&A

Q: From time to time, I will receive a question by email from a customer about a contract, a service visit or our company requirements for a particular awards program. These emails are stand-alone questions and I resolve them in one or two email exchanges. Can I delete the emails promptly since they aren't part of a larger project or deliverable?

A: No. Each exchange you have with a customer can be considered its own Final Business Record and should be retained according to the Record Retention Schedule, regardless of whether it fits within a larger project. You may delete the early emails in the exchange as duplicative so long as the final retained email exchange includes the entire communication thread without any omissions or changes. Even brief email exchanges constitute Final Business Records and should not be deleted until their Retention Period has expired under this Policy. Your Business Unit may have rules about how and where to retain such customer exchanges to ensure their proper retention. Consult your manager to determine the proper Business Unit filing procedure.

2.3 Holds

Information, whether electronic or paper and regardless of content, may be subject to a Hold, as discussed in Section 5 below. No Information subject to a Hold shall be subject to Disposal until the Hold is released.

2.4 Disposal

Information that is not required to be retained under this Policy or a Hold is subject to Disposal. The process for Disposal of Information will depend on the type of file (printed or digital), as well as the contents of the Information. Disposal of Confidential, Highly Confidential and Restricted Confidential Information and Privileged Information is described in Sections 3 and 4 of this Policy. Disposal of other Information no longer required to be retained can be conducted routinely by depositing paper files into trash or shredding bins or by deleting digital files. Any questions about Disposal methods for particular types of Information may be directed to your manager or your Business Unit Ethics & Compliance Officer.

2.5 Instant Messaging (**"IM"**), Text Message (**"Texts"**) and Social Media Usage

Our company e-mail system and company-owned or company-controlled social media platforms are approved channels for business communication and for creating and transferring Information. In addition to company-provided email, other communication channels may be currently available to you or may be developed in the future. These tools, apps, and platforms can be novel and cutting edge, but they are not authorized by Realogy to conduct business.

2.5.1 IM

Depending on your Business Unit, you may now have access to IM through Realogy's computer networks and may use it to communicate with colleagues. Based on the casual nature of IM, however, Realogy has not approved its use for official business communications. Instead, the use of IM has been provided to allow unofficial, non-business communications with colleagues.

Under Realogy's current policy, unless your Business Unit records and retains IM communications, you must not create, store or distribute Information on IM. If you are contacted for business purposes through IM, you should guide the communications back to Realogy's approved communication channels, if appropriate, or speak to the other party in person or on the telephone.

The following additional policies govern the use of IM:

- Not every Business Unit or department within a given Business Unit permits the use of IM tools. You must first determine if the use of IM tools is permitted and if so, use only those IM tools permitted by the Business Unit.
- If offered by the Business Unit, IM is allowed only for transmitting and receiving information that falls into the Non-Record category. It must not be used for any type of communication that would ever constitute Work in Progress or a Final Business Record.
- You may not attach any file to an IM as it may indicate that the communication is of a nature more consistent with a Work in Progress or Final Business Record.

Realogy has the right to retain and review all IM communications conducted through company-provided IM tools at any time.

2.5.2 Other Communication Channels (Texts, Social Media, Apps)

In addition to IM, there are a variety of other communication channels that are available for personal communications that are not appropriate for business use. For example, your smart phone likely provides texting capability and access to other communication apps offered by third party developers. And the number of social media platforms that provide broad and assorted communication tools for users, like Facebook, Twitter and Instagram, continues to grow.

Although these channels continue to multiply, we need to remain mindful of our responsibilities to create, organize and store Information in places it can be accessed and retrieved by our company. Texts and other communication apps are not approved methods for communicating or creating Information. In addition, your personal social media accounts are not approved for creating, distributing or maintaining Information. These communication channels, as well as any later developed communication platforms that are not provided by Realogy for business, are considered **"Non-Approved Channels."** You must not create, store or distribute Information on Non-Approved Channels. If you are contacted for business purposes through a Non-Approved Channel, you should guide the communications back to Realogy's approved communication channels: corporate email accounts and social media pages and accounts controlled by Realogy.

If you use a Non-Approved Channel to conduct Realogy business, subject to applicable law, Realogy will have the right to review your devices (including personal devices) and accounts for the Non-Approved Channel for Information, including a search of data associated with the account and physical access to the device, SIM card or other applicable hardware that contains or may contain Information. Subject to applicable law, you acknowledge that your unauthorized use of Non-Approved Channels to create, communicate or store Information grants Realogy the right to retrieve the Information through the reasonable means described in this Section and the Mobile Technology Policy and its FAQs.

Make a habit out of directing and keeping Information on Realogy Information Technology Resources (like company email) and company platforms to avoid exposing your personal devices, apps and social media accounts to Realogy review and access.

Q&A

Q: One of my important customers regularly asks me business questions over text messages. We speak regularly on our mobile phones and I think he just feels more comfortable using text rather than email. How can I direct my customer to use one form of communication over another?

A: It's tricky. It's never easy to dictate terms to your customers, but it will likely be easier than the alternative. Your communications with Realogy customers over text mean that Realogy Information is stored on your mobile device as opposed to the company's servers. If we later need Information related to that customer, your phone would be at issue and where legally permitted, you might be required to turn it or its SIM card over for review. We want to avoid that situation, if possible.

We recommend speaking with the customer. Let him know that the company has information management policies that require all written communications to be done by email so we can preserve them as required by law. You should stress that the policy protects the Information and communications for both sides and ensures that all of our communications are reflected in our files. Our customers likely understand the challenges of digital information and may even appreciate the company's rules around texting. If the issue persists, speak with your manager to determine if there is another way to address the issue.

3.0 Protected Information

Whether a Work in Progress or a Final Business Record, Information may be further classified if its content is required to be protected under this Policy or the law. Realogy uses three distinct classifications to ensure proper treatment of confidential Information: "Confidential," "Highly Confidential" and "Restricted Confidential" (collectively, **"Protected Information"**). We are each responsible under this Policy for managing the Protected Information we create or control appropriately according to its applicable confidentiality classification.

3.1 Classifications

3.1.1 "Confidential Information" is Information that is proprietary to Realogy and that Realogy chooses not to share or release for circulation beyond certain authorized individuals. Examples of Confidential Information are marketing plans, sales data and certain client or vendor lists.

3.1.2 "Highly Confidential Information" is Information that is intended for a limited group of individuals and, if disclosed, could jeopardize important Realogy interests or actions with serious adverse financial, regulatory or reputational consequences. Examples of Highly Confidential Information can include certain pricing or negotiated contract information, business goals, merger or acquisition plans, systems configurations and code, audit reports, or customer lists with contract termination dates.

3.1.3 "Restricted Confidential Information" is any Information that is subject to laws that forbid or limit unauthorized disclosure of Information. Examples include health information, as well as some Personal Information elements like Social Security numbers, driver's license numbers, birthdates or credit card numbers (also referred to in the U.S. as **"Personally Identifiable Information"** or **"PII"**). Personal Information (as defined below), whether of our customers, vendors, employees or clients, can be viewed as Restricted Confidential Information if its disclosure could result in regulatory or customer notification requirements or a significant increased risk of identity theft or fraud, or if the Personal Information is otherwise considered highly private under applicable law.

Personal Information

"Personal Information" is a broad category of Information that we handle in the course of doing business with and on behalf of our customers, clients, franchisees, employees, independent contractors, vendors and suppliers. The broadest definition of Personal Information is any Information that uniquely identifies an individual. Personal Information is often defined differently in the different jurisdictions – states, countries or territories – where we operate or where the identified individual resides. Examples of Personal Information can include basic Information such as name, telephone number or even email address, as well as Information like financial, credit or health information or information that could be used to steal a person's identity – such as driver's license or government identification numbers. Certain demographic information, including gender, education or political affiliation, when combined with Personal Information, also becomes Personal Information. Laws governing Personal Information, including its definition and treatment, vary by jurisdiction.

Personal Information (cont'd)

United States

In the United States, federal and state laws define Personal Information differently. Realogy follows all applicable U.S. state laws in protecting the following Personal Information (commonly referred to as "PII") as Restricted Confidential Information, regardless of where we receive the Information or where the identified individual resides:

An individual's name **plus** any of the following elements:

- birthdate
- government-issued identification number (e.g., social security number, passport number, driver's license number)
- payment card numbers (e.g., credit card, debit card plus PIN)
- financial account information (savings, checking or investment account numbers)

In addition, any protected health Information (PHI) related to a person will be considered Restricted Confidential Information, including Information about a person's past, present or future physical or mental health, health care services or health care payments. All Restricted Confidential Information must always be handled with care to prevent unauthorized disclosure of Personal Information and PHI, identity theft and liability.

Outside the United States

In addition, for persons living outside the United States, Information that can be used to identify them such as **name, address, contact information or photos** may be considered Personal Information that must be handled and transferred according to the laws of the jurisdiction where the identified individual resides. Consult with your Legal department if you are collecting Personal Information about individuals residing outside the United States – including employees, franchisees, real estate sales associates, vendors, suppliers or customers – to understand the limitations on and protections required for such Personal Information. Further, in some jurisdictions outside the U.S., Information related to political activities, unions and religious affiliations are considered **"Sensitive Personal Information"** that must be treated according to the laws of the applicable jurisdiction. Contact your Legal department immediately if you are collecting Sensitive Personal Information related to political activities, unions and religious affiliations to discuss the business need for and the proper handling of this Sensitive Personal Information.

Outside of Protected Information, you may also have Information related to your work that is considered **"Public."** Information classified as Public is made available outside our company and does not require any special protection or categorization as required for Confidential, Highly Confidential or Restricted Confidential Information. Examples of Public Information are periodicals, published press releases or sales brochures or our published disclosure documents.

3.3 Use and Maintenance of Protected Information

In the course of business activity, you may create, receive or otherwise come in contact with Protected Information. You have a duty to safeguard Protected Information according to this Policy, the Information Security Policy and applicable laws. Protected Information may be contained in Works in Progress or Final Business Records.

We must secure and limit distribution of and access to Highly Confidential Information and Restricted Confidential Information. Access to Protected Information must be strictly limited to those employees and service providers that have a need for Protected Information to perform the authorized functions of their jobs. Service providers (those persons not directly employed by Realogy or its subsidiaries) must be bound to confidentiality in their agreements with Realogy before they can be granted access to Protected Information. In addition, service providers will be required to sign Realogy's Policy on Acceptable Use of Realogy Information Technology Resources for Non-Employees available here.

Any Protected Information, whether in digital or printed form, must be maintained in a secure manner. For more information on proper handling of Protected Information, consult Realogy's Information Security Policy.

3.4 Disposal of Protected Information

At such time as Disposal is appropriate according to this Policy, the Record Retention Schedule and the Information Security Policy, Protected Information maintained in an electronic form must be deleted or destroyed so it is rendered unusable or irretrievable. Protected Information maintained on portable media such as CDs, DVDs, flash drives or other later-developed media devices must be deposited in either a standard shredding bin or a special media shredding bin (for larger volumes of portable media) when Disposal is appropriate. Protected Information maintained on hard drives and the like must be disposed of by IT. Protected Information maintained in paper format and appropriate for Disposal must be shredded.

3.5 Marking of Protected Information Documents

Confidential Information distributed outside of Realogy and all Highly Confidential and Restricted Confidential Information, regardless of distribution, must be clearly marked with the appropriate confidential classification. If you are involved in creating or editing a document that will constitute Protected Information, you must identify the document using the appropriate classification in a header or footer to be repeated on each page of the document for clarity.

Q&A:

Q: My manager and I are working on an Excel spreadsheet for our operations team that contains the names of all of our customers with their contract termination dates. I received the spreadsheet from my manager by email and it is not marked with any designation for confidentiality. Can I assume that the Information is not considered Protected Information?

A: No. Even the best document managers make mistakes. Just because your manager or even a higher level executive fails to properly mark a document does not mean the Information does not need protection. The Information you describe falls squarely within the definition of Highly Confidential Information and the document should be marked in the header or footer of the document. You should discuss this issue with your manager, mark the document, and protect its Highly Confidential Information by limiting distribution of the spreadsheet to those with a need to know.

4.0 Privileged Information

You may create, receive or otherwise come in contact with Privileged Information. **"Privileged Information"** is a communication made between an attorney and client in confidence for the purpose of seeking, obtaining, or providing legal assistance. Information provided to an attorney \\by his client or agent to outline underlying facts for the question or basis for legal advice is also Privileged Information. Further, communications between an attorney, client or agent prepared in connection with, or in anticipation of, litigation or government action is Privileged Information. Privileged Information is protected from discovery or disclosure in certain contexts.

You have a duty to protect Privileged Information under this Policy. Privileged Information cannot be shared with any persons outside the group designated by counsel, and any emails containing Privileged Information cannot be forwarded. Privileged Information may be contained in Works in Progress or Final Business Records. Any Privileged Information, whether in electronic or printed form, must be maintained in a secure manner, with access limited as authorized by in-house counsel. Under no circumstances should Privileged Information be forwarded or distributed outside of Realogy. If you have any questions about handling or distributing Privileged Information, consult with your Business Unit Legal department.

If any Privileged Information is appropriate for Disposal, it will be disposed of as if it contained Protected Information (as described in Section 3.4).

All Privileged Information must be clearly marked as Privileged by including the words "Attorney-Client Privileged Communication" or "Privileged and Confidential." Your Business Unit Legal department or outside legal counsel may designate a preferred method or language for marking Privileged Information.

Q&A

Q: I received a Hold notice on a matter in litigation. I'm not a lawyer but I want to send an email to my colleague (who is not a lawyer) to go over the facts of the case so I can be sure I'm recalling it correctly. Since I know we have retained legal counsel and this matter is with our litigation team, can I send an email marked "Privileged" to my colleague and protect its contents from disclosure?

A: No. The attorney-client privilege exists to protect communications between a lawyer and client. If neither you nor your colleague is a lawyer for the company, your email will not be considered privileged even if you mark it so. Any document or email you create for this purpose may be subject to discovery and disclosure to the other party. You should consult with the Legal department about any concerns you have and about the limits of attorney-client privilege before proceeding with an email or other communications about the case.

5.0 Hold Management

When Information is sought or is reasonably likely to be sought in a threatened or actual litigation or government proceeding, Realogy is legally required to immediately suspend all regularly scheduled or permitted Disposal of related or potentially related Works in Progress and Final Business Records. In order to help ensure that all Information necessary for a matter is preserved, a Hold is issued.

A **"Hold"** is a mandate issued by the Legal department to preserve particular Information that may be needed. When you receive a Hold, you must immediately acknowledge receipt of the Hold and suspend the Disposal of Information related or potentially related to the actual or threatened litigation, government proceeding or audit. Information subject to a Hold must be handled with care. It is a violation of this Policy and the law to alter, destroy or conceal any Information being sought or likely to be sought in a litigation, government proceeding or audit.

5.1 When Does a Hold Take Effect?

Once a Hold is issued for a matter, no Information potentially related to the Hold can be destroyed unless or until specific instructions are issued releasing the Hold. The Senior Vice President of Litigation and Regulatory Affairs has oversight responsibility in connection with the issuance, re-issuance and release of all Holds.

You may receive a Hold notice by email and you must follow the instructions to acknowledge the content of the Hold. If, however, you become personally aware of an anticipated, threatened or actual litigation or government proceeding before receiving a Hold, you have a duty to preserve all related Information and seek guidance from the Legal department even though the official Hold has not yet issued.

You are strictly prohibited from disposing, discarding, withholding or altering Information under Hold. Any such conduct may impede, obstruct or influence any threatened or actual litigation,

governmental proceeding or audit and may expose Realogy to fines, penalties and sanctions regardless of your intent. In addition, such conduct is a violation of this Policy and will be grounds for discipline.

5.2 Content and Execution of Holds

Holds describe the class and parameters of Information that must be preserved. Holds will be sent to you if you may have related or potentially related Information. Holds must be communicated to all custodians of related or potentially related Information, both paper-based and electronic, including individuals in the Information Technology and Information Security departments.

Holds are issued by an attorney or an authorized member of the Legal department **("Hold Issuers"**). The Hold Issuer must also send Holds to any custodians who maintain related or potentially related Information.

Once you are identified as being affected by a Hold, the Hold Issuer will communicate with you and you must confirm your receipt of such communication. Such communication and acknowledgement typically occur by email through Realogy's automated legal hold compliance system (**"Legal Hold System"**).

You are required to act promptly and preserve all related and potentially related Information and to provide such Information, as and when directed by the Hold Issuer. A member of the Legal department may contact you to determine if you have related or potentially related Information and to collect such Information.

The Hold Issuer will regularly remind you of your Hold obligations typically through the legal Hold system.

5.3 Temporary Nature of Holds

Holds may only be lifted or modified in writing by the Hold Issuer as soon as the matter creating the need to preserve is complete or the requirements of the special circumstance have been fulfilled. Even if the matter giving rise to the Hold is resolved, you continue to be subject to the Hold until notified in writing that the duty to preserve is no longer applicable (the **"Hold Release"**).

Holds may not be used to designate Information as "permanent" or to deviate unnecessarily from the Record Retention Schedule. A Hold Release will be issued promptly after the requirements of the special circumstances that gave rise to the Hold have been fulfilled.

The Legal department will monitor and periodically review active Holds to ensure that Holds remain appropriate. You will receive periodic emails from the Legal Hold System containing a link to a personalized summary of all Holds issued to you, including the status of each Hold – i.e. whether it is still in effect or has been released. The Legal department can also provide a summary link at any time upon request; the summary link to the Legal Hold System remains active so you can review your personalized Hold summary at any time.

5.4 Documenting the Hold

Through the Legal Hold System, Hold Issuers will document the (i) imposition, (ii) communication, (iii) implementation, (iv) re-issuance, and (v) release of their Holds.

The documentation will include the basis for the issuance of the Hold, the list of custodians to which the Hold was disseminated, the substantiation of the initial and reissued Holds (e.g., the distribution e-mails), and the communication of the Hold Release.

The documentation of the Hold must be maintained according to the Record Retention Schedule.

Q&A

Q: I receive Holds from time to time and acknowledge receipt in the system. But I continue to manage my email inbox and delete emails I don't need because I assume the company can retrieve anything it needs from the servers. If my email includes communications governed by the Hold, am I in compliance with the Hold notice?

A: No. You are violating the company's policies for record retention and Holds management under this Policy. If you receive a Hold notice, you are required to act personally to retain Information under your control. You are not permitted to rely on other people, processes or systems to retain the Information you receive. The company may face significant penalties and sanctions in court if it is unable to produce particular documents because an employee failed to follow the Hold policy. Do not rely on our servers or other backup mechanisms to meet your obligations to retain Information under a Hold.

6.0 Storage and Disposal of Paper Information

Under the Records Retention Schedule, Realogy requires the storage and retention of certain types of Information. When the Information is contained in physical files, it may make sense to store the Information in an offsite storage facility if the files are no longer needed for day-to-day access. Realogy contracts with Iron Mountain to store our physical files offsite in a secure facility. Your Business Unit may use a different provider, but Iron Mountain is preferred.

The storage of files at an offsite facility allows Realogy to meet its Record Retention Schedule obligations without maintaining physical files at our office locations. It does, however, require you to manage the following additional responsibilities:

- Records prepared for offsite storage must be properly and particularly indexed before they can be transferred offsite to ensure that Realogy personnel can identify them and access them if they are needed. Every file included in a box must be reflected in a written index.

- The index for any offsite storage must be maintained in a central location or shared drive to allow for access by Record Managers and the Legal department.

- Files that pass their Record Retention Period must be affirmatively reviewed and approved for Disposal. Storing files offsite does not automatically put them in line for destruction under our Records Retention Schedule. Your department must continue to review the offsite storage index to identify for Disposal any Information with an expired Record Retention Period (not subject to a Hold) and direct our storage facility to dispose of the Information.

Offsite storage of dated material no longer necessary for day-to-day access is a responsible way to keep our office facilities free of unnecessary files and to protect Information as it awaits its Disposal date under the Record Retention Schedule.

7.0 Vital Records

"Vital Records" are records, which would have a serious or material adverse impact on the ability of Realogy or its Business Units, collectively or individually, to operate following a disaster or emergency if they are lost. Whether designated as Works in Progress or Final Business Records, Information that is necessary for the continuation of our business is considered Realogy's Vital Records. Within each Business Unit, department managers and Business Unit leaders will designate certain records and Realogy Information Technology Resources as Vital Records in the Business Unit business continuity policy.

Vital Records constitute a small percentage of Realogy's overall records, but the importance of these records to the company's ongoing business operations requires additional protection and security.

While many of Realogy's Vital Records are created and maintained on Realogy Information Technology Resources, Vital Records may also be found in other systems and formats, including paper records. Realogy's Corporate and Business Unit Ethics & Compliance Officers are responsible for the process of identifying Vital Records by version and format and must include designations specific to that record prior to storage. Custodians of Vital Records must ensure their protection and preservation according to this Policy and the Information Security Policy.

8.0 Roles and Responsibilities

8.1 Department Responsibilities

Each department within any Realogy Business Unit bears responsibility for managing the Information it creates, uses and controls. Within each department, the Department Manager has an obligation to ensure that Information is handled properly and that procedures are in place to control the production, maintenance, use, and access to the Information. The roles and responsibilities of the Department Manager may be delegated, but overall accountability for the department's compliance with this Policy remains with the Department Manager.

8.2 Individual Roles and Responsibilities

Department Managers will ensure that appropriate controls are in place in compliance with this Policy and the Information Security Policy to manage, handle, label, store, transport and control Information (digital and hard copy) based on (a) the type of Information, (b) whether it is Protected Information, and (c) whether it is a Vital Record. Each Realogy employee must manage the creation, use, retention and ultimate Disposal of Works in Progress and Final Business Records according to the Policy. Each employee must preserve Information subject to a Hold. Additional Information management roles and responsibilities are defined in this Section.

(a) Department Managers

In connection with this Policy, each Department Manager must:

- Monitor and ensure that Business Unit Information is managed under this Policy
- Periodically review the classifications of Information resources under his or her control
- Ensure that department procedures align with this Policy to preserve Business Unit Information subject to Holds
- Oversee the process for off-site storage, Disposal and Quarterly Information Management Week
- Take appropriate steps to ensure that non-employees are informed of their duties and obligations under this Policy

(b) Chief Ethics & Compliance Officer

The Chief Ethics & Compliance Officer will:

- Oversee formulation, implementation and improvement of the Policy
- Approve any exceptions to the Policy
- Coordinate internal communications, marketing and awareness programs related to the Policy
- Provide training related to the Policy
- Support and consult with Business Unit Ethics & Compliance Officers, Deputy Business Unit Ethics & Compliance Officers (as applicable), Department Managers and Record Managers about the Policy
- Ensure that the Policy continues to meet legal requirements

(c) Legal

Individuals with oversight of legal functions at Realogy – including all Business Unit Ethics & Compliance Officers and those persons who manage litigation and regulatory affairs – are responsible for:

- Administering and enforcing the Policy
- Periodic review of Record Retention Schedule requirements

- Designating Hold Issuers
- Authorizing the execution of Holds to preserve Information needed to support litigation, regulatory matters and audits
- Collecting all Information subject to a Hold, whether in paper or electronic format, if applicable
- Periodically reissuing Holds to refresh understanding of the Information to be held
- Authorizing the removal of a Hold when the event that gave rise to the Hold is complete or moot
- Documenting the imposition, communication, implementation, reissue and release of Holds
- Notifying the Chief Ethics & Compliance Officer of any material changes in corporate organization or law that might necessitate an amendment to the Policy

(d) **Record Managers**

Record Managers are appointed by the Ethics & Compliance department to be local leaders in Policy implementation across Realogy. Record Managers have the following responsibilities:

- Act as liaison to the Chief Ethics & Compliance Officer and Business Unit Ethics & Compliance Officer to institute and enforce the Policy
- Assist in training about the Policy
- Ensure that Information is maintained in a manner that makes it identifiable and available for easy access by authorized employees, as necessary
- Oversee record coordinators within the Business Unit that execute day-to-day responsibility for Information Management
- Ensure that Final Business Records and Vital Records are properly indexed and classified
- Ensure that Final Business Records and Vital Records are sent to offsite storage when appropriate
- Grant system access and resolve service matters with storage and shredding vendors
- Provide guidance during Quarterly Information Management Week and establish protocols to encourage the ongoing Disposal of materials appropriate for Disposal and not subject to a Hold

(e) Realogy Employees and Non-Employees

Each Realogy employee and non-employee with access to Information or Realogy Information Technology Resources is responsible for complying with this Policy consistent with law and with Realogy's culture of ethics and integrity, including:

- Keeping Confidential, Highly Confidential, Restricted Confidential, and Privileged Information safe from unauthorized access or disclosure and in compliance with Realogy's Information Security Policy

- Maintaining his or her workstation, work place, or office and electronic files, including e-mail, in an orderly, secure manner to ensure that no Protected Information or Privileged Information is exposed
- Classifying and marking Information appropriately under the Policy
- Exercising due care to help ensure Information can be found when needed, whether stored on-site or off-site, in paper or electronic form. Such care requires, among other things, setting up orderly and sensible directories and files to allow Information to be securely stored and efficiently retrieved when necessary
- Disposing of all Work in Progress no longer needed for business or legal purposes according to the Disposal procedures in this Policy, unless subject to a Hold
- Promptly acknowledging receipt of all Holds issued to them
- Disposing of all Non-Records on a regular basis
- Properly identifying and preserving Final Business Records for off-site storage, retention and Disposal
- Ensuring that all Holds applicable to them are carried out appropriately and that no Information, whether electronic or paper, is disposed of that is subject to a Hold

9.0 Policy Compliance Audits

As part of this Policy various departments and corporate functions will be subject to audit for compliance with the current version of the Policy. Failure to comply with this Policy or other provisions of the Policy could lead to disciplinary or legal action against individuals who fail to comply.

10.0 Risk Policy Requirements

Compliance with this Policy is mandatory. Exceptions to this Policy may be granted by the Chief Ethics & Compliance Officer.

Appendix A -- Definitions

"Active Lives" refers to the number of years an agreement, policy or other document remains in effect for purposes of the Record Retention Schedule, also referred to as the term of an agreement.

"Business Units" refer to the four Realogy Business Units – Realogy Franchise Group, NRT, Title Resource Group and Cartus – as well the Corporate Services Group.

"Confidential Information" is Information that is proprietary to Realogy and that Realogy chooses not to share or release for circulation beyond certain authorized individuals. Examples of Confidential Information are marketing plans, sales data and certain client or vendor lists.

"Department Manager" is a person within a Business Unit designated with managerial and/or operational responsibility over a particular department.

"Disposal" is the process of deletion or disposal of Works in Progress that are no longer needed for current work and Final Business Records that have aged beyond the defined Retention Period. Disposal must be undertaken on a daily basis. Time must also be set aside time for Disposal during Quarterly Information Management Week. No Information subject to a Hold shall undergo Disposal.

A **"Final Business Record"** is Information that represents a final project deliverable or it could be a document or digital file – correspondence, email or other documents – that records our business activities in the ordinary course. Final Business Records must be retained for legal and business reasons for a defined period of time under the Record Retention Schedule. Examples of Final Business Records are executed contracts, correspondence, business email (including final email chains that document all discussion threads), memos, performance appraisals, audit reports, year-end financials, balance sheets, social media campaigns, versions of websites and Realogy training materials.

"Highly Confidential Information" is Information that is intended for a limited group of individuals and, if disclosed, could jeopardize important Realogy interests or actions with serious adverse financial, regulatory or reputational consequences. Examples of Highly Confidential Information can include certain pricing or negotiated contract information, business goals, merger or acquisition plans, systems configurations and code, audit reports, or customer lists with contract termination dates.

A **"Hold"** is a mandate issued by the Legal department to preserve particular Information that may be needed. When you receive a Hold, you must immediately suspend the Disposal of Information related or potentially related to the actual or threatened litigation, government proceeding or audit. Information subject to a Hold must be handled with care. It is a violation of this Policy and the law to alter, destroy or conceal any Information being sought or likely to be sought in a litigation, government proceeding or audit.

"Hold Issuers" are those individuals in the Legal department with the authority to issue Holds.

A **"Hold Release"** is a written notice sent by the Hold Issuer to the custodians named in the Hold that advises the custodians that the duty to preserve is no longer applicable.

"Information" is defined broadly as data in any form (printed or digital) created by, owned or licensed by or entrusted to Realogy.

"IM" refers to the Instant Messaging tool provided through Realogy's computer networks that some Realogy Business Units permit employees to use to communicate with colleagues. Certain Business Units may not permit use of IM. Check your Business Unit rules.

"Legal Hold System" refers to Realogy's automated legal hold compliance system (currently Exterro Fusion Legal Hold for all Business Units except Cartus) that allows Hold Issuers to send notice of Holds and Hold Releases to custodians and allows custodians to acknowledge receipt of Hold notices.

A **"Non-Approved Channel"** refers to communication channels, such as IM, Text, personal social media accounts, and any later developed communication platforms, that are not approved by Realogy for creating, storing or distributing Information.

A **"Non-Record"** is a document or digital file that is personal in nature, has no retention value for the company or does not involve any business transacted on behalf of the company. A Non-Record may include personal emails, calendar notes, casual messages that do not relate to Realogy business, or incidental work reference materials. Non-Records do not constitute Information under this Policy.

"Personal Information" is a broad category of Information that we handle in the course of doing business with and on behalf of our customers, clients, franchisees, employees, independent contractors, vendors and suppliers. The broadest definition of Personal Information is any Information that uniquely identifies an individual. Personal Information may be defined differently in the different jurisdictions – states, countries or territories – where we operate or where the identified individual resides. Examples of Personal Information can include financial, credit or health information or information that could be used to steal a person's identity (commonly referred to in the U.S. as "Personally Identifiable Information" or "PII") – such as driver's license or government identification numbers. Certain demographic information, including gender, education or political affiliation, when combined with Personal Information, also becomes Personal Information in some jurisdictions. Laws governing Personal Information definition and treatment vary by jurisdiction.

"Policy" means this Information Management Policy, as well as the Record Retention Schedule, which is incorporated into this Policy.

"Privileged Information" is a communication made between an attorney and client in confidence for the purpose of seeking, obtaining, or providing legal assistance. Information provided to an attorney by his client or agent to outline underlying facts for the question or basis for legal advice is also Privileged Information. Further, communications between an attorney, client or agent prepared in connection with, or in anticipation of, litigation or government action is Privileged Information. Privileged Information is protected from discovery or disclosure in certain contexts. For example, the advice or guidance from any attorney who represents

Realogy, whether written or verbal, is Privileged Information and may not be disseminated or disclosed to any other person, except as authorized by Realogy in-house counsel on a need-to-know basis. This type of Information must be handled with care to avoid an inadvertent waiver of the privilege (i.e., the unauthorized disclosure of Privileged Information may cause the waiver or loss of the privileged qualities of that communication). The decision to waive privilege can only be made with the advice of in-house counsel. Information with any level of confidentiality may be Privileged Information. For further guidance on the principles of attorney-client communications or attorney work product, contact an attorney from the Legal department as the privilege laws may vary significantly in each country where Realogy operates.

"Protected Information" means any Information classified under one of the following three distinct classifications to ensure proper treatment of Information: "Confidential," "Highly Confidential" and "Restricted Confidential."

"Public" is defined, with respect to Information, as Information that made available outside our company and does not require any special protection or categorization as required for Confidential, Highly Confidential or Restricted Confidential Information. Examples of Public Information are periodicals, published press releases or sales brochures or our published disclosure documents.

"Quarterly Information Management Week" is the formal process, conducted four times a year, through which employees set aside time to review Information and perform Information management duties. This includes the identification and storage of Final Business Records. It also includes the Disposal of Works in Progress that are no longer needed for current work, and Final Business Records that have aged beyond the defined Retention Period. No Information subject to a Hold shall be subject to Disposal.

"Realogy Information Technology Resources" refers, but is not limited, to networks and servers, email and website platforms, desktop PCs, laptops, tablets, databases, mobile phones, smart phones, printing devices, telephones, facsimile machines, Realogy-controlled social media platforms, voicemail systems and any other electronic device capable of storing or transmitting information, including e-mail, instant messaging and Internet access provided by Realogy. The software installed on such devices and resources is also included. Realogy Information Technology Resources may also refer to non-Realogy host or server computers, stand-alone computers, laptops and any other communication devices, software, data files and networks when used to perform Realogy business.

"Record Managers" are designated employees within Realogy Business Units who are appointed by the Ethics & Compliance department to be local leaders in the implementation of this Policy.

"Record Retention Schedule" is part of this Policy and defines record categories and Retention Periods. The Realogy Record Retention Schedule is maintained at http://athome.realogy.com. The Record Retention Schedule defines business record categories by business function, and identifies the applicable Retention Period for each of the countries in which Realogy conducts business.

"Restricted Confidential Information" is any Information that is subject to laws that forbid or limit unauthorized disclosure of Information. Examples include certain information such as health information, as well as some Personal Information elements like Social Security numbers, driver's license numbers, birthdates or credit card numbers. Personal Information, whether of our customers, vendors, employees or clients, can be viewed as Restricted Confidential if its disclosure could result in regulatory or customer notification requirements or a significant increased risk of identity theft or fraud, or if the Personal Information is otherwise considered highly private under applicable law.

"Retention Period" is the length of time Final Business Records identified in the Record Retention Schedule must be preserved. Retention Periods may be stated in terms of years, or may be expressed as contingent upon the occurrence of an event such as the termination of a contract. For most record types, the Retention Period begins when a Final Business Record is identified.

"Sensitive Personal Information" is a designation used in some jurisdictions outside the U.S. – in the European Union, for example – to refer to Information related to an individual's political activities, unions and/or religious affiliations. The collection, security and use of Sensitive Personal Information must comply with all applicable laws.

"Texts" are text messages, SMS messages or other direct message formats available directly or through software applications on mobile devices. Texts are considered Non-Approved Channels and are not permitted for creation, storage or distribution of Information.

"Vital Records" are records, which would have a serious or material adverse impact on the ability of Realogy or its Business Units, collectively or individually, to operate following a disaster or emergency if they are lost. Whether designated as Works in Progress or Final Business Records, Information that is necessary for the continuation of our business is considered Realogy's Vital Records. Within each Business Unit, department managers and Business Unit leaders will designate certain records and Realogy Information Technology Resources as Vital Records in the department and Business Unit business continuity policy.

A **"Work in Progress"** is Information created for a particular project or assignment that must be retained for the duration of the project or assignment on Realogy's behalf. If any Information is needed for ongoing work – even if the work extends for several months or years – that Information is considered a Work in Progress. Examples of a Work in Progress are drafts, duplicates, project plans, notes, work papers, support documents, working files, duplicate emails in ongoing email chains, and informal correspondence related to work/project activities. A Work in Progress will usually culminate in a Final Business Record with the successful completion of a project or assignment, or if the project is unsuccessful, a Work in Progress may become the Final Business Record for purposes of this Policy.