The Respect Trust Framework™

VERSION 2.1 – 2016-02-01

Single Page Summary

Purpose

The purpose of the Respect Trust Framework is to define a set of principles and rules to which all Members of a digital trust network agree so that they may share Member Information with confidence that its privacy will be protected and it will only be used as authorized.

Principles

Principle	Synopsis	Wording
Promise	*We will respect each other's digital boundaries*	Every Member promises to respect the right of every other Member to control the Member Information they share within the network and the communications they receive within the network.
Permission	*We will negotiate with each other in good faith*	As part of this promise, every Member agrees that all sharing of Member Information and sending of communications will be by permission, and to be honest, direct and fair about the purpose(s) for which permission is sought.
Protection	*We will protect the identity and data entrusted to us*	As part of this promise, every Member agrees to provide reasonable protection for the privacy and security of Member Information shared with that Member.
Portability	*We will support other Members' freedom of movement*	As part of this promise, every Member agrees that if it hosts Member Information on behalf of another Member, the right to possess, access, control, and share the hosted information, including the right to move it to another host, belongs to the hosted Member.
Proof	*We will reasonably cooperate for the good of all Members*	As part of this promise, every Member agrees to share the reputation metadata necessary for the health of the network, including feedback about compliance with this trust framework, and to not engage in any practices intended to game or subvert the reputation system.

Rules

The Respect Trust Framework is made self-reinforcing through use of a peer-to-peer reputation system for both positive reputation and negative reputation. The rules for this are defined in a subdocument called The Respect Reputation System™.

The Respect Promise™

The Respect Promise is the contractual commitment made by and among Members upon joining the network that establishes mutual duties and benefits among all Members as expressed by the statement: "*I promise to uphold the purpose, principles, and rules of the Respect Trust Framework.*"

Table of Contents

Status: Version 2.1

This version of the Respect Trust Framework was submitted by Respect Network Corporation on 1 February 2016 for public listing with the Open Identity Exchange (OIX)[1] as a digital trust framework in accordance with the Open Identity Trust Framework (OITF) Model.[2] As the name implies, OIX is an open exchange on which trust frameworks are listed for public inspection and usage by different market participants. The Respect Trust Framework was specifically developed to address the market need for an increase in the level of control that all legal persons (both individuals and Organisations) have over their digital identity and personal and private data.

Respect Network Corporation serves as the provider of the Respect Network™, which incorporates the Respect Trust Framework into its Member contract. The Respect Trust Framework may only be modified by trusted members of the Respect Network as provided for in the Versioning and Amendments section of this document. This ensures that future evolution of the Respect Trust Framework only happens with the input and consent of the Members, a requirement which fulfills the Open Versioning Principle, one of the twelve Principles of Openness as defined in the OITF Model.

As described in the Local Terms section of this document, each Member of the Respect Network has the authority to decide the local terms that apply to specific relationships with other Members provided they do not conflict with the global terms defined in this Respect Trust Framework. This applies to Respect Network Corporation as well, i.e., Respect Network Corporation as the network provider is subject to the Respect Trust Framework in the same way as every other Member.

The first Public Review Version of the Respect Trust Framework was submitted to OIX on 10 May 2011. Following the feedback and suggestions received during the public review period, Version 1 Beta was submitted to OIX on 15 August 2011 to become the first operational version for use with Connect.Me, the first product produced under the Respect Trust Framework. This first version carried the designation "Beta" because it was expected to continue to evolve based on feedback and suggestions received during the early growth period of Connect.Me. The next version, Version 1 Beta 2, with minor revisions regarding operational policies, was submitted to OIX on 29 February 2012.

Version 2 was submitted to OIX on 23 June 2014. This version separates out the Respect Reputation System and the FIPPS into subdocuments, and adds two additional subdocuments: the Respect Business Framework and the Technical and Operational Specifications.

Version 2.1 was submitted to OIX on 1 February 2016. This version updated the Respect Business Framework and elided the Version 2.0 Technical and Operational Specifications.

[1] http://www.openidentityexchange.org/
[2] http://www.openidentityexchange.org/sites/default/files/the-open-identity-trust-framework-model-2010-03.pdf

Subdocuments

This version of the Respect Trust Framework includes four subdocuments that are published independently but incorporated by reference into this master document. Each of these subdocuments is versioned independently; the latest version shall always be the one legally in force.

The Respect Reputation System™

Defines the peer-to-peer reputation system that implements the Proof Principle of the Respect Trust Framework

The Respect Business Framework™

Defines the business rules of the Respect Trust Framework.

Mapping of the Respect Principles to Fair Information Practices Principles

Provides a mapping between the Respect Principles and Fair Information Practices Principles as defined by different governing bodies around the world.

Definitions

This document and all subdocuments of the Respect Trust Framework share the following definitions. Subdocuments may also define additional terms specific to that subdocument.

1. **Respect Network** is the network of interdependent rights and duties relationships formed by all parties who agree to be bound by the Respect Trust Framework, including the integrated business, legal and technical rules governing participation.
2. **Member** means any legal person (e.g., individual, commercial, governmental, etc.) that has joined the Respect Network and contractually agreed to the Respect Promise.
3. **Member Account** means the unique account representing a Member as a unique legal person on the Respect Network.
4. **Member Information** means the personal data and identity information controlled by a Member, including data, text, graphics, videos, or other content and materials, for sharing within the Respect Network under the terms of the Respect Trust Framework. For purposes of this definition, the term "controlled by" means sourced from or shared by the Member.
5. **Member-Sourced Information** means Member Information for which the Member is the original source through which such data and information was included in the Respect Network.
6. **Member-Shared Information** means Member Information for which the Member is not the original source through which such data and information was included in the Respect Network, but for which the Member has been authorized to provide access or distribute within the Respect Network consistent with the Respect Trust Framework.
7. **Individual Member** (also called **Personal Member**) means a Member who joins as a natural person representing only himself/herself and not another legal entity.
8. **Individual Membership** means the Respect Network membership owned by an Individual Member.
9. **Organisational Member** (also called **Business Member**) means a Member that joins in any legal capacity other than as an Individual Member.
10. **Organisational Membership** means the Respect Network membership owned by an Organisational Member.
11. **Cloud Name** means a human-friendly reassignable XDI address registered by a Member.
12. **Cloud Number** means a machine-friendly persistent XDI address registered by a Member.
13. **XDI (Extensble Data Interchange)** means the open standard for semantic data interchange defined by the OASIS XDI Technical Committee.
14. **Context** means a uniquely addressable digital representation of a semantic concept with which Members may associate their Member Information. A Context is labeled with a Tag. A Context may also be labeled with a visual icon or graphic.
15. **Tag** means a human readable semantic label for a Context. Multiple tags that are semantically equivalent, either in the same human language or in different human languages, may be assigned to the same Context.
16. **Community** means the set of Members and Member Information associated with a specific Context.

17. **Vouch** means a signal of positive reputation in a specific Context made by one Member about another Member.
18. **Complaint** means a signal of negative reputation in any Context made by one Member about another Member.
19. **Voucher** means the Member making a Vouch.
20. **Complainant** means the Member making a Complaint.
21. **Recipient** means the Member that is the subject of a Vouch or a Complaint.
22. **Trust Level** means an indicator of the level of expectation that a Member will abide by his/her Respect Promise. Each Trust Level has a set of requirements a Member must meet to achieve that Trust Level as defined in the Trust Levels section below.
23. **Trust Anchor** means the highest Trust Level as defined in the Trust Levels section below.
24. **Connection** means a relationship established through the Respect Network between two Members for the purposes of communicating or sharing Member Information.
25. **Connection Request** means a message sent from one Member to another Member to request the creation of a Connection.
26. **Inappropriate Connection Request** means a Connection Request that, *in the sole judgment of the Member receiving it,* is not respectful of the receiving Member's time and attention.
27. **Verified Connection** means a Connection whose existence has been digitally verified by the Respect Reputation System.
28. **Private Connection** means a Connection whose existence is not publicly discoverable.
29. **Public Connection** means a Connection whose existence is publicly discoverable.
30. **Trust Anchor Connection** means a Verified Connection in which one Member is vouching for another Member as a Trust Anchor.
31. **Reputation Graph** is the metadata describing a Member that is maintained by the Respect Reputation System to represent the reputation of that Member.
32. **Profile** is the specific view of Member Information and the associated Reputation Graph available to other Members in a specific Context, or to the public if the Profile is public.
33. **Persona** is a representation of a Member's digital identity controlled by that Member.
34. **Dashboard** is the interface a Member is provided for setting preferences and sending and receiving communications through the Respect Network.

Purpose

The purpose of the Respect Trust Framework is to define a set of principles and rules to which all Members of a digital trust network agree so that they may share Member Information with confidence that its privacy will be protected and it will only be used as authorized.

Principles

Following are the five fundamental principles upon which the Respect Trust Framework is based:

Principle	Synopsis	Wording
Promise	*We will respect each other's digital boundaries*	Every Member promises to respect the right of every other Member to control the Member Information they share within the network and the communications they receive within the network.
Permission	*We will negotiate with each other*	As part of this promise, every Member agrees that all sharing of Member Information and sending of communications will be by permission, and to be honest, direct, and fair about the purpose(s) for which permission is sought.
Protection	*We will protect the identity and data entrusted to us*	As part of this promise, every Member agrees to provide reasonable protection for the privacy and security of Member Information shared with that Member.
Portability	*We will support each other Member's freedom of movement*	As part of this promise, every Member agrees that if it hosts Member Information on behalf of another Member, the right to possess, access, control, and share the hosted information, including the right to move it to another host, belongs to the hosted Member.
Proof	*We will reasonably cooperate for the good of all Members*	As part of this promise, every Member agrees to share the reputation metadata necessary for the health of the network, including feedback about compliance with this trust framework, and to not engage in any practices intended to game or subvert the reputation system.

These principles, called the Respect Principles, were extracted from the common elements of privacy, data protection, and trust across different jurisdictions and legal traditions around the world. The Respect Trust Framework includes a subdocument, *Mapping of the Respect Principles to Fair Information Practices Principles ("FIPPs Mapping")*, that provides a chart that matches the Respect Principles with different versions of Fair Information Practices Principles (FIPPs) from different countries and international Organisations, as well as with common law principles.

The following sections provide further guidance to understanding and interpreting each Respect Principle, including examples of the "duties of care" for handling of Member Information consistent with each principle. The guidance below is intended to be normative, i.e., it is intended to be relied upon directly in the application and interpretation of the Respect Trust Framework. The examples provided are intended for illustrative (informative) purposes only.

Like the examples, the FIPPs Mapping sets forth additional guidance for application of the Respect Principles that is intended to be merely informative, not normative. In the case of the FIPPs Mapping , it is recognized that authority for existing FIPPs may vary from one legal jurisdiction to another. The chart in FIPPs Mapping illustrates specifically how the Respect Principles relate to a subset of current legal authorities. More generally, the individual FIPPs associated with each Respect Principle provide examples of the types of specific duties that are intended to be covered by each Respect Principle, and thereby they collectively help to inform how the Respect Principles may be interpreted.

Notably, most FIPPs were developed to cover the needs of only individual data subjects (primarily in the context of data collections by governmental and commercial parties). The Respect Principles are broader, intending to support the identity integrity of all data subjects, whether individual, commercial, governmental, or otherwise. As a result, existing FIPPs should be consulted with the understanding that they need to be broadened to cover all entities, not just individuals.

The Promise Principle

> ***Promise.*** *Every Member promises and agrees to respect the right of every other Member to control the Member Information they share within the network and the communications they receive within the network.*

The Promise Principle represents each Member's agreement to be bound by the duty to respect each other Member's online "identity integrity" in all circumstances, even without being asked by another Member to do so.

Without the respect by outside parties of a person's "boundaries," their identity has uncertain integrity, which is perceived by an individual person as a lack of privacy and security, and by a legal entity as a lack of security and increased liability risk. Just as people and entities in the physical world need protection from "trespass," "unreasonable searches and seizures," unauthorized access, and other physical and perceptual intrusions, individuals and legal entities need to be able to maintain identity integrity against similar intrusions online.

The Promise Principle is directed at causing Members to adopt the duties, in their role as data handlers, to respect other Members' online identity integrity. The duties are directed toward data flows in two directions. Identity integrity is proportional to the degree to which a data subject has control of both their inputs (what data and communications they receive) and outputs (how data from them and information about them observed by others is distributed). Both are covered in the Promise Principle.

The common law privacy tort of "unreasonable intrusion upon another's seclusion" is a traditional root of this Principle. Not all international jurisdictions embrace that particular concept in law, but each has some concept of the legal boundaries that separate one legal entity from another. By making the promise in the Promise Principle, each Member is simply stating that they will respect those legal boundaries, consistent with local customs, local law, *and* the Respect Trust Framework. A breach of duty under the Promise Principle to respect identity integrity generally constitutes an intrusion on identity integrity under the Respect Trust Framework. A subset of those Respect Trust Framework intrusions includes those legally cognizable as torts, crimes, and civil rights violations.

Another way to view this Principle is as an instantiation in digital terms of the ethic of reciprocity widely known as "The Golden Rule." In essence, the first Principle represents the duty of each Member to "*treat data about others as you would like them to treat data about you".*

So fundamental is this Principle to the Respect Trust Framework that the other four principles are all stated as extensions to this principle.

In addition, this Principle also represents the contractual commitment all Members are making to other Members when they join a trust network such as the Respect Network operating under the Respect Trust Framework. For this reason it is referred to with the trademarked name **The Respect Promise™**. This is explicitly defined to mean:

> "*I promise to uphold the purpose, principles, and rules of the Respect Trust Framework*."

The Permission Principle

> ***Permission.*** *As part of this promise, every Member agrees that all sharing of Member Information and sending of communications will be by permission, and to be honest, direct, and fair about the purpose(s) for which permission is sought.*

The Permission Principle clarifies that one specific aspect of each Member's duty to respect the integrity of each other Member's digital boundaries is by seeking permission to "cross" them, i.e., to specifically request consent from another Member to use shared data or to send communications, and to do so with an honest and clear statement of the purposes of the request.

While the Promise Principle sets up a default duty of non-intrusion (*aka* respect for identity integrity), the Permission Principle anticipates that what would otherwise be an "intrusion" may be authorized with "permission" when that permission is fairly and reasonably sought. Such permission is inherently granted when a Member explicitly approves of a relationship or transaction with another Member and the Member Information being requested falls within the natural social or business context of that relationship or transaction. Separate permission must be requested from and explicitly granted by the Member for any use of that Member's Information that falls outside of the natural social or business context of the approved relationship or transaction.

Examples of harms resulting from violation of the Permission Principle in the physical world are characterized as the traditional torts and legal "causes of action" referred to as "infringement," "conversion," "misappropriation," "violation of publicity rights," and "unjust enrichment." All of these involve harms to a person from use of or intrusion upon their likeness, name, property or other rights without their permission frequently (but not exclusively) for third party monetary gain. Similarly, individuals and legal entities operating online should be asked for permission for certain uses of their identity and personal data.

Like the Promise Principle, the duties in the Permission Principle are directed towards data flows for both incoming and outgoing transfers of data and communications across the identity "boundary." These two directions of transfer relate to two separate traditional common law privacy torts. The Permission Principle's duty to obtain permission for "all sharing of identity and personal data," is similar to the duties associated with the common law tort of "misappropriation." The duty to obtain permission for *sending* of communications *to* a Member is intended to prevent the separate harm of "unreasonable intrusion upon another's seclusion."

The Permission Principle is related to the Promise Principle, but reflects a different set of duties. The Permission Principle recognizes that the identity integrity established in the Promise Principle is not an impermeable barrier, but needs to be recognized as a "semi-permeable membrane", i.e., one that permits data and communications to flow to and from Members. The Permission Principle simply requires that Members be involved in the decisions about how data flows to and from them, and that permission about those flows be obtained openly, honestly and fairly.

The Protection Principle

> ***Protection**. As part of this promise, every Member agrees to provide reasonable protection for the privacy and security of the Member Information shared with that Member.*

The Protection Principle represents each Member's agreement to be bound by the duty to protect identity and personal data shared with that Member, specifically against unauthorized intrusions of a third party.

People in the physical world who depend on others to protect them from third party harm also need protection from harm caused by the failure of those others to perform those duties. In the physical world, this "duty to protect" varies greatly from one context to another, since the harms to be protected against also vary. There are many types of traditional legal actions that can result from a breach of duty to protect another person in various contexts. The more general, multi-context, legal concepts of "detrimental reliance" and "negligence" were developed to deal with the broader issues of compensating parties that are harmed because another party breached a duty to protect. In the latter case, the establishment of a duty (including a duty to protect someone's person or property) could lead to liability for the person bound by the duty if such person breached the duty in a way that caused damages (such as when a hired security guard falls asleep on the job, allowing a robbery to take place).

The Protection Principle relates to the traditional common law privacy torts of unreasonable publicity disclosing details of another's private life, and to negligence.

The Portability Principle

> ***Portability**: As part of this promise, every Member agrees that if it hosts Member Information on behalf of another Member, the right to possess, access, control, and share the hosted information, including the right to move it to another host, belongs to the hosted Member..*

The Portability Principle represents each Member's agreement to be bound by the duty to cause any Member Information shared with that Member to be portable, i.e., to be available to the data subject Member to easily copy or move to other contexts of the Member's choosing.

Just as people in the physical world need to be able to move about freely, and to be protected from limitation of movement characterized in extreme cases as "kidnapping," and "false imprisonment," individuals and legal entities need to be able to access and share their digital identity and data about them online from a variety of services and in a variety of contexts. The Portability Principle is directed at causing Members, in their role as data collectors and handlers, to respect other Members' online identity integrity by granting such access.

The traditional harms of "false imprisonment" and "kidnapping" and, in the consumer rights context, "lack of consumer choice" are the roots of this principle.

The Proof Principle

> ***Proof**: As part of this promise, every Member agrees to share the reputation metadata necessary for the health of the network, including feedback about compliance with this trust framework, and to not engage in any practices intended to game or subvert the reputation system.*

The first four Respect Principles relate primarily to duties involving actions taken with respect to identity and personal data, whereas the Proof Principle focuses on maintaining information flows needed for operation of a reputation system that provides incentive for all Members to abide by, and encourage other Members to abide by, these Principles.

People in the physical world need protection from the harm to reputation called "defamation" and its twin torts "libel" (written defamation) and "slander" (spoken defamation). There is also the related common law privacy tort called "False Light," where reputation is harmed by the juxtaposition of identity information about a person with other unrelated information that causes the impression of a relationship that can harm the person's reputation.

The Proof Principle creates a duty for all Members of the trust network to cooperate as peers in maintaining their reputations in order to prevent these same harms online.

Local Terms

The Respect Trust Framework is intended to establish a set of terms that apply globally to all relationships and exchanges of personal data that take place between Members through the Respect Network ("Global Terms"). For some relationships or exchanges these Global Terms may be sufficient. For other relationships or exchanges these Global Terms may need to be supplemented by other terms specific to a particular relationship or exchange ("Local Terms"). Examples of Local Terms include terms-of-service agreements, localized privacy policies, specialized security policies, and other context-specific policies. Local Terms may be part of Plug-In Trust Frameworks (see below), or they may be more limited, stand-alone sets of Local Terms.

By joining the Respect Network, a Member agrees that the Local Terms the Member requires for any relationship or exchange with other Members will not conflict with, or require an alternative interpretation of, the Global Terms of the Respect Trust Framework. (This rule also applies to Respect Network Corporation itself, as explained in the Status section above.)

Plug-In Trust Frameworks

The Respect Trust Framework is intended to provide a global set of principles and rules for protection of identity and personal and private data on a digital trust network. Groups of Members may desire to develop more specific sets of principles and rules applicable to more specific domains while still maintaining compatibility with the Respect Trust Framework. Such sets of principles and rules are called **Plug-In Trust Frameworks**. For a trust framework to normatively cross-reference the Respect Trust Framework as a Plug-in Trust Framework, it must meet the following rules:

1. It must provide an explicit reference to the current version of the Respect Trust Framework.
2. It must not define principles or rules that are in conflict with, or requiring an alternate interpretation of, the principles or rules defined in the Respect Trust Framework.

Versioning and Amendments

Given that the purpose of the Respect Trust Framework is to engender trust among Members of a digital trust network, it is of utmost importance that the Members be able to rely on the integrity and stability of the trust framework itself. For this reason, until such time as the Respect Network reaches a population of at least one million Trust Anchors, Respect Network Corporation may make only such amendments as may reasonably shown to be in the best interests of all Members. After such time as the Respect Network reaches a population of at least one million Trust Anchors, any amendments to this main document of the Respect Trust Framework may only be approved by the Trust Anchors according to the following rules.

1. All Trust Anchors shall receive formal notice of the vote ("Voting Notice") from Respect Network Corporation via an electronic message delivered to their Dashboard including a

link to an electronic ballot with relevant information about the proposed amendment. This is the only way an amendment to the Respect Trust Framework may be initiated.

2. All Trust Anchors as of the time Voting Notice is issued shall be eligible to vote on the amendment. No other Members are eligible to vote.
3. The Voting Notice shall be made at least thirty calendar days prior to the deadline by which a ballot must be submitted ("Voting Deadline") to permit Trust Anchors time to read, study, and debate the amendment.
4. Each Trust Anchor shall be allocated 100 votes.
5. A Trust Anchor may vote all of their own votes, or may assign any portion of their 100 votes to one or more other Trust Anchors to vote as their proxy, or any combination of these options. Proxies will only be recognized if established through official Respect Network Corporation voting proxy processes.
6. There is no required quorum.
7. An amendment shall pass if, after passage of the Voting Deadline, it has received equal to or greater than a two-thirds supermajority of the votes cast. Otherwise it shall fail.
8. If the amendment passes, Respect Network Corporation shall post and announce the amended version of the Respect Trust Framework to all Members within five business days. The terms of the amended version shall be effective 30 days after the announcement.

Respect Network Corporation may only make amendments to all subdocuments of this main document as may reasonably shown to be in the best interests of all Members.

Copyrights and Trademarks

Respect Network Corporation
12233 Corliss Avenue North, Seattle, WA 98133, USA