American Red Cross

Protecting Personal Information Policy

Status	**Final**
Policy ID	1005
Responsible Office	Office of General Counsel
Sponsor	Privacy Officer
Policy Interdependencies (if any)	Information Security Policy (P1012)

1. Purpose

The purpose of the Policy on Protecting Personal Information is to describe the principles the American Red Cross follows in safeguarding the personal information it receives from clients, donors, employees, volunteers and other constituents. The Policy expresses the American Red Cross's commitment to privacy and responsible handling of personal data.

This Policy does not establish precise rules and procedures for handling personal information. Instead, each department that collects, handles, or uses personal information must adopt practices and procedures as appropriate to ensure that personal information is protected in accordance with this Policy. When feasible, privacy protections should be incorporated into the design of American Red Cross systems and programs.

2. Scope

This is a corporate-wide Policy and applies to all employees, volunteers and contractors in any Red Cross department or unit. Everyone at the American Red Cross is responsible for safeguarding personal information. Protecting privacy is a value that is integrated into all of our programs and systems.

3. Definitions

Personal Information is any non-public information about an individual that is created or received by the American Red Cross. Personal Information may include an individual's name, address, birth date, telephone number, e-mail address, social security number, financial account numbers (including credit card numbers), biometric identifiers (such as fingerprints), photographs, dates of service, health information, information about financial and blood donations, and other types of data. Some types of Personal Information, such as health information, social security numbers, and other information

that can be used to commit identity theft, are entitled to greater privacy protections than other types of Personal Information.

A **Personal Information Security Breach** occurs when an unauthorized person obtains access to unencrypted Personal Information or an authorized person uses or attempts to use Personal Information in an unauthorized manner.

4. Policy Statement

4.1 Introduction

The American Red Cross is dedicated to the following general principles regarding the protection of Personal Information:

- We will collect and use Personal Information only as needed in support of the American Red Cross mission and our humanitarian activities.
- We will protect Personal Information from improper use or disclosure.
- We will comply with applicable privacy and data security laws.

4.2 Privacy Officer

The Privacy Officer, an attorney who reports to the General Counsel, addresses privacy-related issues that arise out of American Red Cross activities. Among other things, the Privacy Officer is responsible for maintaining this Policy on Protecting Personal Information and providing instruction and guidance regarding implementation of and compliance with legal privacy requirements.

The Privacy Officer coordinates privacy-related activities with the Chief Information Security Officer. The Chief Information Security Officer reports to the Chief Information Officer and is responsible for ensuring the safeguarding of Personal Information as it is processed, stored and transmitted across American Red Cross technology resources. The Privacy Officer and the Chief Information Security Officer lead the organization's response to Personal Information Security Breaches.

4.3 Employee and Volunteer Commitment to Privacy

Every employee and volunteer of the American Red Cross must adhere to this Policy on Protecting Personal Information and the privacy procedures and practices that apply to his or her American Red Cross activities. Every employee and volunteer must sign the American Red Cross *Code of Business Ethics and Conduct* and *Confidential Information and Intellectual Property Agreement*, confirming that they will not use or disclose confidential information obtained as a result of their American Red Cross work except as authorized.

4.4 Collection of Personal Information

The American Red Cross may collect Personal Information only as needed to provide services and conduct activities in support of the American Red Cross mission and humanitarian services.

4.5 Persons Granted Access to Personal Information

American Red Cross employees and volunteers may have access to Personal Information only as needed to perform their job functions. An independent contractor, leased worker, consultant, temporary employee, vendor or provider of services may have access to Personal Information only as needed to perform duties on behalf of the American Red Cross and only after agreeing in writing to implement reasonable practices and procedures to protect the privacy of Personal Information.

4.6 Use of Personal Information

Personal Information may be used within the American Red Cross only as needed to provide services and conduct legitimate American Red Cross activities.

4.7 Maintenance, Storage and Security of Personal Information

Prudent and reasonable precautions must be taken to maintain and store Personal Information in a secure manner. These precautious must include physical, electronic and procedural safeguards, as appropriate, to prevent unauthorized access to systems and locations where Personal Information is stored.

Access to files, databases, and computers containing Personal Information must be limited to authorized persons. Personal Information maintained in electronic format must be password protected. Enhanced levels of protection, including encryption, may be necessary in some circumstances. Personal Information should not be maintained in an electronic shared file or directory unless access is limited to authorized persons.

Documents, laptops, mobile devices and other items containing Personal Information may be removed from the business premises of the American Red Cross only as authorized and only if American Red Cross staff maintains complete control and supervision over the items. Additionally, American Red Cross staff must ensure that access to the Personal Information therein is limited to authorized persons.

4.8 Disclosure of Personal Information

The American Red Cross protects Personal Information from unauthorized disclosure. In certain circumstances, however, Personal Information may be disclosed to comply with the law, benefit clients or communities served by the American Red Cross, or advance the American Red Cross humanitarian mission. Each unit and department of the

American Red Cross must ensure that any disclosure of Personal Information is appropriate and consistent with legal obligations. Examples of situations in which disclosure may be appropriate, depending upon the circumstances, include the following:

- The subject of the Personal Information or the subject's authorized representative has consented to disclosure;
- Disclosure is necessary to avert a threat to the health or safety of another person or the community;
- Disclosure is necessary to detect, prevent or otherwise address fraud or crime against the American Red Cross or on the business premises of the American Red Cross;
- Disclosure is required by law, including:
    - subpoenas, court orders and warrants;
    - laws and regulations requiring disclosure of information to a regulatory agency such as the Food and Drug Administration;
    - laws and regulations requiring disclosure to public health authorities for the purpose of preventing or controlling disease, injury, disability or death; and
    - laws requiring medical and social service professionals to report suspected neglect, abuse or criminal activities;
- American Red Cross senior management, upon consultation with the Privacy Officer and/or Chief Information Security Officer as appropriate, authorizes disclosure.

When authorized, disclosure of Personal Information may be made only to the extent necessary to accomplish the purpose of the disclosure.

Nothing in this Policy is intended to prohibit employees from engaging in protected concerted activity, such as speaking, writing, or communicating with fellow employees or others about their wages, benefits or other terms of employment.

4.9 Privacy-Related Security Breaches

Every actual or suspected Personal Information Security Breach must be promptly reported to the Privacy Officer and Chief Information Security Officer. The Privacy Officer and Chief Information Security Officer will work with other personnel and departments as appropriate to identify the Personal Information that may have been compromised and investigate the circumstances surrounding the breach. They will determine any actions necessary to address the breach, comply with the law, and minimize the potential for loss to the American Red Cross or the persons whose Personal Information was compromised.

4.10 Social Security Numbers and Financial Account Numbers

Because social security numbers, driver's license numbers, and credit and debit card numbers and other financial account numbers can be used in the commission of identity theft, American Red Cross units and departments must minimize their collection and retention of such information. Where it is necessary to maintain such information, strong security controls must be used to prevent unauthorized individuals from accessing the information.

Social security numbers, credit and debit card numbers, and other financial account numbers may not be publicly posted or displayed, nor may they be printed or embedded on any card required to access American Red Cross products or services. In addition, individuals may not be required to transmit such information over the Internet unless the connection is secure or the numbers are encrypted. Such information should not be visible on the outside of any materials transmitted by mail.

5. Enforcement Responsibility

The head of each unit or department is responsible for (a) protecting the privacy of Personal Information used in the unit or department's activities in accordance with this Policy on Protecting Personal Information, (b) complying with any applicable privacy laws, and (c) developing procedures and practices as necessary to fulfill these responsibilities.

6. Implementation and Communication

The Policy will be implemented and/or communicated to the organization making use of email, the Exchange, and corporate communications such as *Cross Connection*. It will be referenced in new employee orientation and various training sessions.

7. Source of Authority/Legislative Context

Various state and federal laws impose requirements on the collection, maintenance and use of certain types of personal information, including but not limited to social security numbers, credit card numbers, and blood donor information. In addition, on September 28, 2007, the Board of Governors adopted the Resolution on the Confidentiality of Personal Information.

8. Associated Documents

Issues regarding the maintenance, storage and security of Personal Information in electronic form are also addressed in the Information Security Policy (P1012).