

## Standards of Conduct

### 1. Confidential or Proprietary Information

You may become aware of confidential or proprietary information (“**Confidential Information**”) about CSRF’s business. Confidential Information means information which is special or unique to CSRF, information which CSRF has undertaken to protect as confidential or proprietary and/or information which is required to be maintained as confidential by law or regulation. Information regarding CSRF finances or Personal Information of its employees, contractors, members, clients, Americanism Program recipients and Scholarship applicants and recipients is CSRF’s Confidential Information. “**Personal Information**” means information which personally identifies an individual.

You are obligated to keep all Confidential Information confidential forever. You may disclose or use the minimum amount of Confidential Information which is needed to perform your duties and, then, in accordance with CSRF policies including but not limited to the CSRF Privacy Policy posted at: [[casr-foundation.org](http://casr-foundation.org)] and all applicable laws and regulations. You may disclose Confidential Information to those having a need to know and who are under an appropriate obligation of confidentiality which may require a non-disclosure agreement or other written consent be in effect.

Do not accept information from employees or 3<sup>rd</sup> parties that may be sensitive or confidential in nature if you do not have a need to know to carry out your assigned duties. Familiarize yourself with the Privacy Policy.

### 2. General Precautions.

- Take care to avoid having your discussion overheard.
- Do not leave Confidential Information in plain view taking special care to clean whiteboards, keep Confidential Information you are not using off your desktop and do not leave any Confidential Information on the photocopier or fax.
- If appropriate, clearly mark files and correspondence as *Confidential*.
- Mail or electronic mail (email) marked as “confidential” or “proprietary” should only be opened or accessed by the person to whom it is addressed.
- The server room should be accessed only by authorized individuals.
- File cabinets including Confidential Information should be locked at all times with access permitted only by those having a need to know and who are authorized.
- Do not share passwords.
- Shred all Confidential Information.

**Use of Systems and Devices.** Take care that systems and devices used to conduct CSRF business do not permit unauthorized access to or use of Confidential Information or CSRF networks, systems or devices.

### 3. Notify the Point of Contact in your Center if you:

- Receive a request to disclose Confidential Information by subpoena, other court order or process,
- Have reason to suspect or believe there has been an unauthorized use or disclosure of Confidential Information, or
- Receive a request to change, amend, modify Personal Information.

**The unauthorized use or disclosure of Confidential Information by employees or board members may result in discipline up to and including termination. Contractors, volunteers and students may be terminated. In addition, violators may be subject to personal civil or criminal liability.**

**Contact Kristin Hoffman with any questions or comments regarding this Standards of Conduct or the CASRF Privacy Policy.**

Acknowledged and agreed to, voluntarily, freely and knowingly, this \_\_\_ day of \_\_\_\_\_, 20\_\_.

\_\_\_\_\_  
Sign Name

\_\_\_\_\_  
Print Name