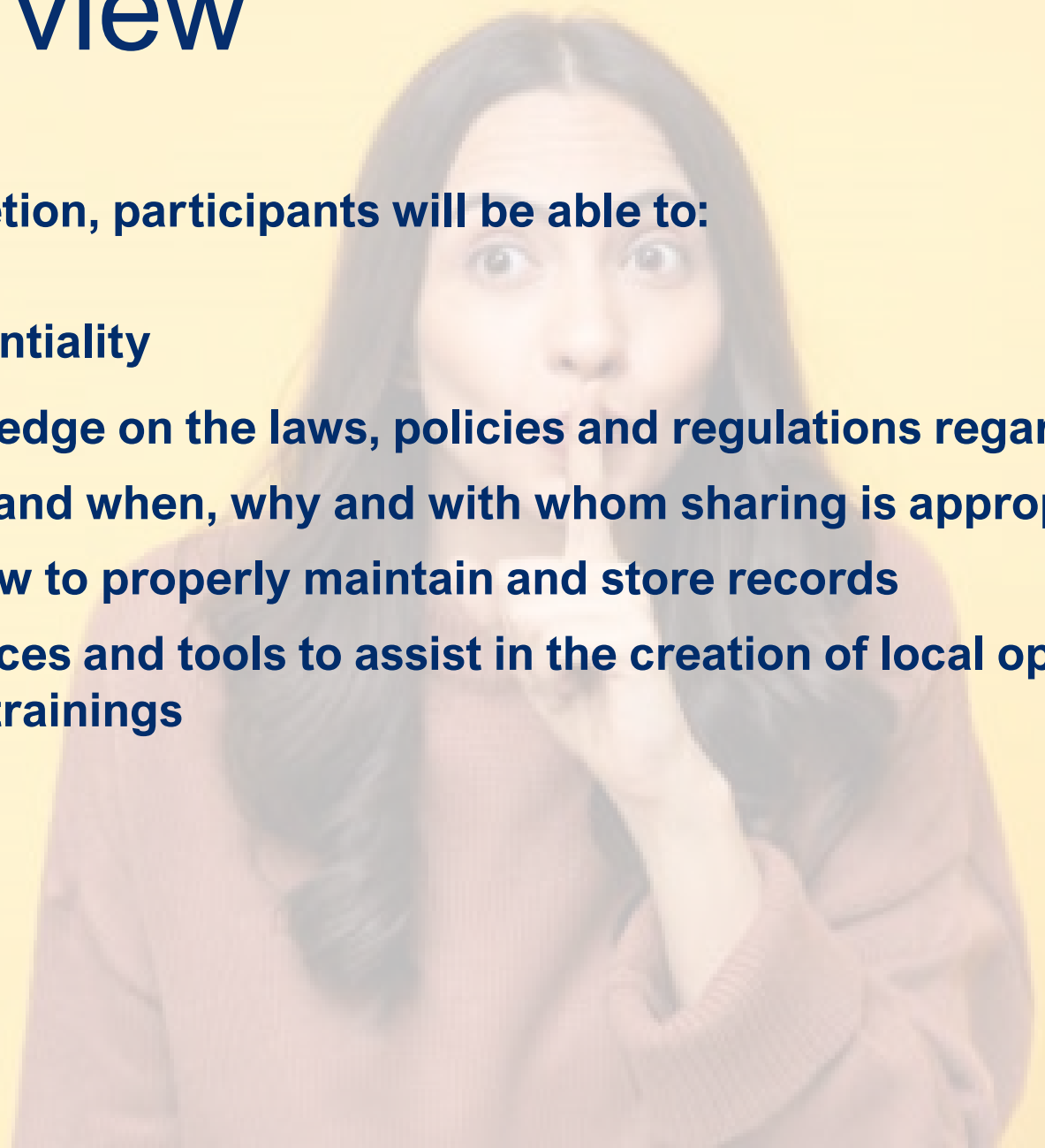
# FY26

# Confidentiality

## Integrity, Security & Trust

# Overview



**Following completion, participants will be able to:**

- **Define Confidentiality**
- **Improve knowledge on the laws, policies and regulations regarding Confidentiality**
- **Better understand when, why and with whom sharing is appropriate**
- **Understand how to properly maintain and store records**
- **Identify resources and tools to assist in the creation of local operating procedures and volunteer trainings**

# Definitions to understand

- **Confidentiality:** The sending, receiving and managing of information to guarantee the safety, security, and integrity of the information is maintained –not illegally disclosing information obtained in confidence
- **Privacy:** The right of each individual to decide when and whether to share personal information, how much information and the circumstances under which information can be shared
- **Personally Identifiable Information (PII):** The information that can be used to distinguish or trace an individual's identity (name, SSN#, biometric records, date of birth, address, contact information, etc.)
- **Non-Disclosure Agreement (NDA):** A legal document to guarantee internal or confidential information is not released, shared or turned over to outside programs, organizations or businesses/companies
- **Subpoena:** A legal request for documents/information served by an attorney
- **De-Identified Information:** Information with enough PII removed or obscured to the degree where the remaining information is not enough to identify an individual
- **Anonymized Information:** Information that has been de-identified AND does not include any type of re-identification code(s)

# Basic Principles

To better understand confidentiality, it is important to have awareness of the four basic principles upon which confidentiality of information is based…

**CONFIDENTIALITY**

- Respect for an individual's right to privacy
- Respect for human relationships in which personal information is shared
- Expectations that those who pledge to safeguard confidential information will do so
- Appreciation of the importance of confidentiality to both individuals and society

Source: "Understanding Confidentiality: Confidentiality Protocol for Handling Issues of Confidentiality in Public Schools." http://www.mbteach.org. Retrieved August 2018.

# Laws & Policies

Impacting confidentiality:

- **Health Insurance Portability and Accountability Act (HIPAA):** A law that protects patients' medical records, and other health information, from release by an individual, business/company, or organization
- **Family Education Rights and Privacy Act (FERPA):** A law that protects the exchanging or releasing of students' records and personal information
- **Child Abuse Prevention and Treatment Act (CAPTA):** Enacted by Congress to create standardized processes and procedures for preventing and responding to child abuse and neglect, while also identifying measures for receiving, managing and responding to allegations of abuse or neglect
- **Children's Online Privacy Protection Act (COPPA):** Requires specific notices be given to users when collecting personal information from children under the age of 13 and establishes and maintains reasonable procedures to protect the confidentiality, security, and integrity of any collected information

Source: United States Department of Justice (DOJ). https://www.justice.gov/. Retrieved August 2018.

# Permitted Disclosure

Certain situations that make it legal to disclose information:

- **Search Warrants & Subpoenas:** Disclosing information as a result of these actions is legal, as the proper steps were taken, and legal protocols were followed
  - *NOTE: Many legal experts advise not immediately turning over information requested as part of a subpoena, as there may be legal action taken in court to either block or amend the original subpoena*
- **Mandatory Reporting:** Disclosing information when filing a report of suspected abuse and/or neglect of a minor or dependent adult to the proper authorities
- **Duty to Warn:** Disclosing information to the proper authorities whenever an individual's actions pose a direct threat to themselves and/or others

Source: "Understanding Confidentiality: Confidentiality Protocol for Handling Issues of Confidentiality in Public Schools." http://www.mbteach.org. Retrieved August 2018.

# LCYPC/CYPC Responsibilities

You have access to all types of PII for youth, families, volunteers and more; understanding the **policies, processes and expectation** for handling PII is a critical and part of your official duty, while also having both **legal** and **ethical** obligations to protect information.

LCYPC/CYPC Statement of Work (SOW) states:

- 10.The CYPC shall **securely maintain** all specified Child & Youth Program **volunteer records**, including specified volunteer **position descriptions, training, and background checks** in accordance with Family Program and Child and Youth Services requirements in AR 608-10, DoDI 6060.4, ARNG CYS Resource Guidance and applicable Chief of National Guard Bureau Memorandums and Instructions
- 29.The CYPC shall **secure and safeguard all Government property, including documents, provided for or created by the operations of Child & Youth Services**. It is understood that all records, documents and resources utilized by the LCYPC, and in support of Child & Youth Services operations are for official Government use only and shall remain Government property on termination of the contract and/or employment

# LCYPC/CYPC Responsibilities

(continued)

You have access to all types of PII for youth, families, volunteers and more; understanding the policies, processes and expectation for handling PII is a critical and part of your official duty.

ARNG CYS Performance Work Statement (PWS=Contract) states:

- 1.4.5.10 Protection of Personally Identifiable Information (PII). **The contractor shall protect all PII encountered in the performance of services in accordance with DF ARS 224.103, Personally Identifiable Information, and DoDD 5400 .11, Department of Defense Privacy Program, and DoD 5400 .11-R**. If a PII breach results from the contractor's violation of the aforementioned policies, the contractor shall bear all notification costs, call-center support costs, and credit monitoring service costs for all individuals whose PII has been compromised.

**It is recommended that you work with your SFPD to clearly identify the types of PII encountered and information can/cannot be divulged – Pay careful attention to both state/territory and national laws*

**Plan and conduct volunteer trainings annually for each volunteer which includes the signing of a Confidentiality Agreements prior to supporting CYS and/or partnered events.**

# Best Practices

To be utilized at **all times** when receiving, storing or sharing PII:

- Ensure computers, laptops, tablets and cell/office phones are secured at all times, especially when not at your workstation (i.e. remove CAC and lock screens)
- Utilize cover sheets to ensure forms are protected from the view of others
- File and secure documents/records in designated and approved storage areas
- Discuss PII in secure and confidential locations – closed door
- Refrain from gossiping or discussing PII about Families/youth in open areas – Avoid gossiping **completely**!
- Ensure any disclosure of PII is done legally as applicable to the situation
- Ensure volunteers sign confidentiality agreements before providing support

# Record Keeping

**Physical Security of Records:** This pertains to how records are to be handled and secured while being used by authorized personnel

**Access to Records:** Not only who has access to the various types of records, but also how information will be encrypted/password protected when exchanging digitally

**Periods of Maintenance for Individual Records:** Timelines and processes for updating records – **WHO** is responsible for **WHAT** and **WHEN**?

**Destruction of Records:** The processes for ensuring the appropriate disposal of information and records (physical copies and digital)

**Storage of Records (Short and Long Term):** Operating procedures for storing records (both short-term and long-term records) – What requires locked security? If stored in a shared space, processes for safeguarding against access by others

**Breech or Release of Information (unauthorized):** Processes and procedures to follow should it become apparent PII has inadvertently been divulged to unauthorized individuals/groups

# Legal & Ethical Obligations

The unauthorized and/or illegal release of PII by CYS staff/Government contractor and the Volunteers you work with can have negative legal & employment consequences.

| Employment Consequences | Legal Consequences |
| --- | --- |
| • Staff member/contractor will face disciplinary action by his/her employer of record<br>• Depending on the severity and impact of the unauthorized release of information, disciplinary action can include a verbal/written counseling notice, up to termination of employment | • Staff member/contractor may face legal action against him/her from the individual(s) whose PII was released without authorization<br>• Staff member/contractor may be held accountable for any harm suffered by the individual as a result of PII being released<br>• Staff member/contractor may face criminal fines or penalties for releasing PII<br>• The future of the CYS Program can be in jeopardy as a result of PII being released |

**Always take appropriate actions to ensure the safety, security and safeguarding of all information on youth, Families, Service Members, volunteers and vested groups and/or individuals**

# Resources

Good for referring to when developing local processes and procedures for safeguarding PII:

- Technology Safety Toolkit: https://www.techsafety.org/confidentiality/
- U.S. Department of Health & Human Services: https://www.hhs.gov/hipaa/for-professionals/training/index.html
- ~~U.S. Department of Education: https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html~~ *As of 23Oct25 site and contents unavailable, check periodically
- American Camp Association: https://www.acacamps.org/resource-library/articles/hipaa-privacy-rule-compliance-%E2%80%94-what-does-it-mean-camps

# Knowledge Assessment

Completion of this online module will be documented by way of a reflective assessment.

To access the reflective assessment, please click on the link below:

https://testmoz.com/q/Confidentiality

Upon completion of the reflective assessment, the National Training Coordinator (NTC) will receive an email with your response included – this will serve as documentation that you successfully completed this module.


# Congratulations!

**You have completed the annually-required (by contract) Confidentiality Module.**

**Thank You!**