

CYBER SAFETY IMPROVEMENT AND PREVENTION FOR YOUTH (CSIPY) CONFIDENTIALITY ACKNOWLEDGEMENT

The Applicant acknowledges that participation in the Cyber Safety Improvement and Prevention for Youth (CSIPY) Grant Program may require the collection, creation, maintenance, transmission, or storage of confidential, sensitive, or personally identifiable information relating to youth, parents, program participants, employees, volunteers, or other individuals.

As a condition of receiving funding, the Applicant agrees to the following:

1. Protection of Confidential Information

The Applicant shall maintain the confidentiality of all personally identifiable information (PII), confidential records, electronic data, and other sensitive information obtained through activities funded under this award.

Confidential information shall be used solely for purposes directly related to the administration of the approved grant-funded project and shall not be disclosed except as authorized by law or with the appropriate written consent of the individual or, when applicable, the individual's parent or legal guardian.

2. Protection of Information Relating to Minors

Because this grant program primarily serves youth under eighteen (18) years of age, the Applicant acknowledges that information identifying minors requires heightened protection. The Applicant shall ensure that any records containing information regarding minors, including but not limited to:

- Names;
- Addresses;
- Telephone numbers;
- Email addresses;
- Photographs;
- School information;
- Online usernames;
- Social media identifiers;
- Internet activity;
- Electronic communications;
- Case records;
- Behavioral information;
- Medical or mental health information; and
- Any other personally identifying information,

are maintained in a secure manner and disclosed only as permitted by applicable federal or Nevada law.

3. Compliance with Nevada Law

The Applicant agrees to comply with all applicable federal, state, and local laws governing privacy, confidentiality, and data security, including but not limited to:

- Nevada Revised Statutes Chapter 239B governing the protection of personal information maintained by governmental entities;

- All applicable Nevada laws governing confidential records involving minors;
- Applicable records retention requirements;
- Applicable data breach notification requirements; and
- Any confidentiality requirements contained within the grant award or Special Conditions.

4. Cybersecurity Requirements

The Applicant agrees to implement reasonable administrative, technical, and physical safeguards designed to protect confidential information from unauthorized access, disclosure, alteration, destruction, ransomware, phishing attacks, malware, or other cybersecurity threats.

At a minimum, the Applicant shall:

- Restrict access to confidential information to authorized personnel;
- Maintain password-protected information systems;
- Utilize multi-factor authentication where available;
- Encrypt confidential electronic information whenever feasible during transmission and storage;
- Maintain current antivirus and security software;
- Regularly update systems with security patches;
- Maintain secure backup procedures; and
- Securely destroy confidential information when retention is no longer required by law.

5. Staff Confidentiality

The Applicant shall ensure that employees, contractors, interns, volunteers, consultants, and subcontractors with access to confidential information:

- Receive training regarding confidentiality and data privacy;
- Understand their legal responsibilities concerning confidential information; and
- Comply with all agency confidentiality policies.

The Applicant remains responsible for any breach of confidentiality by individuals acting on its behalf.

6. Data Sharing

Information collected through this grant shall not be sold, shared, released, published, or otherwise disclosed except:

- As required by law;
- Pursuant to a lawful court order;
- With written authorization from the appropriate individual or legal guardian;
- In aggregate form that does not identify any individual; or
- As required by the Nevada Office of the Attorney General for grant monitoring, auditing, or reporting purposes.

7. Data Breach Notification

The Applicant agrees to immediately notify the Nevada Office of the Attorney General upon discovery of any actual or suspected:

- Unauthorized disclosure;
- Loss of confidential information;
- Cybersecurity incident;
- Ransomware event;

- Compromised user account; or
- Breach involving confidential information collected through this award.

The Applicant shall cooperate fully with any investigation, mitigation efforts, corrective actions, or reporting obligations.

8. Monitoring

The Nevada Office of the Attorney General reserves the right to review the Applicant's confidentiality practices, data security procedures, and record management systems during grant monitoring or site visits.

Failure to maintain adequate safeguards may result in corrective action, suspension of reimbursement, termination of the award, repayment of grant funds, or other remedies permitted by law.

Certification

By signing below, the Applicant certifies that it has read, understands, and agrees to comply with the confidentiality, privacy, and cybersecurity requirements described herein and will ensure compliance by all personnel associated with the funded project.

Agency: _____

Authorized Official: _____

Title: _____

Signature: _____

Date: _____