Privacy Impact Assessment (PIA)

for the

You For Youth Portal Web Application (Y4Y)

April 1, 2021

For PIA Certification Updates Only: This PIA was reviewed on **Enter date** by **Name of reviewer** certifying the information contained here is valid and up to date.

Contact Point

Contact Person/Title: Daryn Hedlund/COR
Contact Email: daryn.hedlund@ed.gov

System Owner

Name/Title: Metasebia Belachew/ISO
Principal Office: Office of Elementary and Secondary Education (OESE)

Please submit completed Privacy Impact Assessments to the Privacy Office at privacysafeguards@ed.gov

*Please complete this **Privacy Impact Assessment (PIA)** on how personally identifiable information (PII) is collected, stored, protected, shared, and managed electronically by your system. You may wish to consult with your ISSO in completing this document.*
If a question does not apply to your system, please answer with N/A.

1. Introduction

1.1. Describe the system including the name, acronym, and a brief description of the program or purpose for the system.

You for Youth (Y4Y) is a website designed to provide professional development learning modules for more than 100,000 after-school professionals in the U.S. Department of Education's (Department's) 21st Century Community Learning Centers (21st CCLCs). The 21st CCLC program is a grant program in which each state receives a grant based on its share of Elementary and Secondary Education Act (ESEA) Title I, Part A funds. States must use their allocations to make competitive awards to eligible entities to operate community learning centers.

The website is an ed.gov public website (y4y.ed.gov) that allows the public to access professional development learning modules. This can be done without registering, although users who register are able to access additional information about after-school activities and programs, sign up for a monthly newsletter of timely topics, and participate in a discussion board and webinars. The discussion board is integrated into the website. The user registration process will allow access to the discussion board. Webinars are conducted on the Zoom platform and recordings are posted to the Y4Y website.

Contact information for Department employees responsible for the 21st CCLC program is posted on the website. Visitors to the website may also provide name and email address to request technical assistance, submit suggestions, and contact the help desk for support.

The system is hosted in the ADTI-GSS hosting environment, a shared service hosting provider for the Department.

1.2. Describe the purpose for which the personally identifiable information (PII)[1] is collected, used, maintained or shared.

[1] The term "personally identifiable information" refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. OMB Circular A-130, page 33

Registration information, including first name, last name, email address, display name, and password, is required to establish accounts, save and track completion progress on courses, participate in the webinars and discussion forums, and enable webinar participants to interact via chatbox, which is a function of the website, during a course.

Additional optional information, such as state, role, job title, and other interests, such as professional development topic areas, is collected for analytical purposes only. Data may be analyzed to better tailor website experience for the users based on their roles and use cases. These data are stored in a database and accessed through an administrative interface.

Name and email address is also collected from users who wish to register for a monthly newsletter, which is managed by Constant Contact, a third-party servicer that supports the Department by distributing a newsletter using an email list.

Name and email address is collected from visitors to the website so that they may request technical assistance, submit suggestions, and contact the help desk for support.

1.3. Is this a new system, or one that is currently in operation?

Currently Operating System

1.4. Is this PIA new, or is it updating a previous version?

Updated PIA
This PIA is being updated as part of regular system assessment activities.

1.5. Is the system operated by the agency or by a contractor?

Contractor

1.5.1. If the system is operated by a contractor, does the contract or other acquisition-related documents include privacy requirements?

☐ N/A

Yes

2. Legal Authorities and Other Requirements

If you are unsure of your legal authority, please contact your program attorney.

2.1. What specific legal authorities and/or agreements permit and regulate the collection and use of data by the system? Please include name and citation of the authority.

The 21st CCLC program is a state formula grant program authorized under Title IV, Part B, of the Elementary and Secondary Education Act, as amended by The Every Student Succeeds Act (ESSA) of 2015 This listed under 20 U.S.C. ch. 28 § 1001 et seq. 20 U.S.C. ch. 70. The ESSA continued the 21st CCLC program as formula grant program in which each State receives a grant based on its share of ESEA Title I, Part A funds. States must use their allocations to make competitive awards to eligible entities. The statute allows the Secretary of Education to reserve up to one percent of the total appropriation for the 21st CCLC program to carry out an array of national activities, such as the Y4Y website.

SORN

2.2. Is the information in this system retrieved by an individual's name or personal identifier such as a Social Security Number or other identification?

No

2.2.1. If the above answer is **YES,** this system will need to be covered by Privacy Act System of Records Notice(s) (SORN(s)).[2] Please provide the SORN name, number, Federal Register citation and link, or indicate that a SORN is in progress.

☑ N/A

Click here to enter text.

2.2.2. If the above answer is **NO**, explain why a SORN was not necessary. For example, the information is not retrieved by an identifier, the information is not maintained in a system of records, or the information is not maintained by the Department, etc.

☑ N/A

The information is not retrieved by unique identifier.

Records Management

[2] A System of Records Notice (SORN) is a formal notice to the public that identifies the purpose for which PII is collected, from whom and what type of PII is collected, how the PII is shared externally (routine uses), and how to access and correct any PII maintained by ED. https://connected.ed.gov/om/Documents/SORN-Process.pdf

If you do not know your records schedule, please consult with your records liaison or send an email to RMHelp@ed.gov

2.3. What is the records retention schedule approved by National Archives and Records Administration (NARA) for the records contained in this system? Please provide all relevant NARA schedule numbers and disposition instructions.

The ED records schedule is 254: Grants Administration and Management Files (N1-441-11-001). Records are destroyed 10 years after last action is taken on the file, but longer retention is authorized if required for business use.

2.4. Is the PII contained in this system disposed of appropriately, and in accordance with the timelines in the records disposition schedule?

Yes

3. Characterization and Use of Information

Collection

3.1. List the specific PII elements (e.g., name, email, address, phone number, date of birth, Social Security, etc.) that the system collects, uses, disseminates, or maintains.

Registration information:

- Required: first name, last name, email address, and password.
- Optional information: state, role, job title, interests, and user-created display name.

Helpdesk/contact form information

- First name, last name, and email address.

3.2. Does the system collect only the minimum amount required to achieve the purpose stated in Question 1.2?

Yes

OESE collects only the minimum information necessary to administer the program. The registration information must be collected to establish accounts, enable users to track completion progress on courses, receive email newsletters, and participate in the

webinars and discussion forums. The optional information is collected for analytical purposes to tailor the website offerings. Name and contact information is required so that the Department can respond to inquiries and requests for assistance, and for users to submit suggestions.

3.3. What are the sources of PII collected (e.g., individual, school, another agency, commercial sources, etc.)?

The PII is collected directly from individuals who visit or register on the website.

3.4. How is the PII collected from the stated sources listed in Question 3.3 (e.g., paper form, web page, database, etc.)?

The PII is collected from the individuals through the registration page on the Y4Y web page or on the contact us webpage.

3.5. How is the PII validated or confirmed to ensure the integrity of the information collected?[3] Is there a frequency at which there are continuous checks to ensure the PII remains valid and accurate?

The registration page has restricted form filling. One example of restricted form filling is that usernames must be at least 5 characters long and emails must have @ included. The PII is not checked beyond the restricted form filling. However, if an email address is invalid, the user will not be able to register and is likely to correct the information.

Use

3.6. Describe how the PII is used to achieve the purpose stated in Question 1.2 above.

Registration information, including first name, last name, email address, display name, and password, is used to establish accounts, save and track completion progress on courses, participate in the webinars and discussion forums, and enable webinar participants to interact by text during a course.

Additional optional information, such as state, role, job title, and interests is used to better tailor website experience for the users based on their roles and use cases.

[3] Examples include restricted form filling, account verification, editing and validating information as it's collected, and communication with the individual whose information it is.

Name and email address is used to enable individuals to register for a monthly newsletter and to enable the Department to provide technical assistance, receive suggestions, and provide help desk support.

3.7. Is the system using PII for testing/researching new applications or information systems prior to deployment or for training employees?

No

3.7.1. If the above answer is **YES,** what controls are in place to minimize the risk and protect the data?

☑ N/A

Click here to enter text.

Social Security Numbers

It is the Department's Policy that, in order to collect Social Security Numbers, the System Owner must state the collection is: 1) authorized by law, 2) necessary for an agency purpose, and 3) there is no reasonable alternative.

3.8. Does the system collect Social Security Numbers? Note that if the system maintains Social Security Numbers but does not explicitly collect them, answer 3.8.1 to address the purpose for maintaining them.

No

3.8.1. If the above answer is **YES**, explain the purpose for its collection, and how the SSN will be used.

☑ N/A

Click here to enter text.

3.8.2. Specify any alternatives considered in the collection of SSNs and why the alternatives were not selected.

☑ N/A

Click here to enter text.

4. Notice

4.1. How does the system provide individuals with notice about the collection of PII prior to its collection (e.g., direct notice, such as a Privacy Act Statement (if applicable) or public notice, such as a SORN, PIA,)? If notice is not provided, explain why not.

A privacy notice is provided on the registration page and this PIA is posted to ed.gov/notices.

4.2. Provide the text of the notice or the link to the webpage where the notice is posted if notice is provided other than by SORN or PIA.

☐ N/A

https://y4y.ed.gov/join/

> You for Youth will collect no personal information about you unless you choose to provide that information to us. We do not give, share, sell or transfer any personal information to a third party. Information collected is used just for analytical purposes and is not used for any other uses. Data may be analyzed to better tailor the website for the users based on their roles and use cases. This information will not be used for any other purposes. Email information may be used to disseminate information about the field based on the expertise area of the registered user. Users can still opt out of the communication if the user desire to choose to do so. Please do not submit any sensitive or personnel information in any of the forms.

4.3. What opportunities are available for individuals to consent to uses (including new uses of previously collected PII), decline to provide PII, or opt out of the project?

Registration is optional. Visitors to the website can access all content on the website without registration. However, to participate in the user forums, receive newsletters, and save and track your training, registration is required.

Users who wish to obtain technical assistance, submit suggestions, and receive help desk support must provide contact information so the Department may provide these services.

4.4. Is the notice referenced in Question 4.1 reviewed and revised when there are changes in the practice, policy, or activities that affect the PII and privacy to ensure that individuals are aware of and can consent to, where feasible, these changes?

Yes

5. Information Sharing and Disclosures

Internal

5.1. Will PII be shared internally with other ED principal offices? If the answer is **NO**, please skip to Question 5.4.

No

5.2. What PII will be shared and with whom?

☑ N/A

Click here to enter text.

5.3. What is the purpose for sharing the specified PII with the specified internal organizations?

☑ N/A

Click here to enter text.

External

5.4. Will the PII contained in the system be shared with external entities (e.g. another agency, school district, the public, etc.)? If the answer is **NO**, please skip to Question 6.1.

No

5.5. What PII will be shared and with whom? List programmatic disclosures only.[4]
Note: If you are sharing Social Security Numbers externally, please specify to whom and for what purpose.

☑ N/A

Click here to enter text.

5.6. What is the purpose for sharing the PII with the specified external entities?

☑ N/A

Click here to enter text.

[4] If this information is covered by Privacy Act System of Records Notice (SORN) please list only relevant programmatic disclosures listed under the Routine Uses section.

5.7. Is the sharing with the external entities authorized?

☑ N/A

Click here to select.

5.8. Is the system able to provide and retain an account of any disclosures made and make it available upon request?

☑ N/A

Click here to select.

5.9. How is the PII shared with the external entity (e.g. email, computer match, encrypted line, etc.)?

☑ N/A

Click here to enter text.

5.10. Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or other type of approved sharing agreement with another agency?

☑ N/A

Click here to select.

5.11. Does the project place limitation on re-disclosure?

☑ N/A

Click here to select.

6. Redress

6.1. What are the procedures that allow individuals to access their own information?

Registered users may access their own profile by logging in to the website.

6.2. What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Registered users may update any of the information that was collected during the registration process via the staffed help desk.

6.3. How does the project notify individuals about the procedures for correcting their information?

Instructions for contacting the help desk to correct information can be found at https://y4y.ed.gov/contact/.

7. Safeguards

If you are unsure which safeguards will apply, please consult with your ISSO.

7.1. Does the principal office work with their CSO/ISSO to build privacy & security into the system and build privacy extensions to the extent feasible?

Yes

7.2. Is an Authority to Operate (ATO) required?

Yes

7.3. Under NIST FIPS Pub. 199, what is the security categorization of the system: **Low, Moderate, or High?**

☐ N/A

Low

7.4. What administrative, technical, and physical safeguards are in place to protect the information?

This system must obtain a signed authorization to operate from a designated Department authorizing official. Youth for Youth Portal (Y4Y) has therefore implemented technical, administrative, and physical privacy and security controls in compliance with the Federal Information Security Modernization Act (FISMA) and with National Institute of Standards and Technology (NIST) standards.

Additionally, Y4Y access is only available to authorized users. Y4Y only supports secure communication protocols for Y4Y users. Personnel in system administration and support roles must successfully complete personnel background screening for at least a moderate risk and complete additional training including role-based, incident response, and disaster recovery training. Physical security of electronic data will be maintained in a secured data center, access to which is controlled by multiple access controls.

System, administration, and security audit logs are reviewed monthly, or more frequently should it be warranted. Furthermore, adverse reporting will be submitted to the agency Information Systems Security Officer (ISSO) and security teams.

When users select a link to go to Constant Contact, the third party that administers the Y4Y newsletter, the Department provides the users with notice that they are leaving the Education Department (ED) environment and are going to the Constant Contact environment. That environment has strong security, a description of which can be found at the Constant Contact webpage.

7.5. Is the information in the system appropriately secured in accordance with the IT security requirements and procedures as required by Federal law and policy?

Yes

7.6. Has a risk assessment been conducted where appropriate security controls to protect against that risk have been identified and implemented?

Yes

7.7. Please describe any monitoring, testing or evaluation conducted on a regular basis to ensure the security controls continue to work properly at safeguarding the PII.

Y4Y will be authorized for operation in accordance with the Department's Security Authorization Program. As part of the authorization to operate granted by the Security Authorization Program, Y4Y will be required to comply with both the current version of NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, and the Department's Information Security Continuous Monitoring Roadmap. Examples of testing and evaluation include routine security assessments that are conducted and validated by the Information Assurance Team, which require vulnerability scans and mitigation of vulnerabilities within the times specified by the Department. System, administration, and security audit logs are reviewed monthly, or more frequently should it be warranted. Adverse reporting will be submitted to the agency ISSO and security teams.

8. Auditing and Accountability

8.1. How does the system owner assess and ensure that the PII is used in accordance with stated practices in this PIA?

The Y4Y system owner is involved in the drafting and reviewing of this PIA and attends all major security and privacy meetings to ensure that PII is only used in accordance with stated practices in this PIA. The system completes the Department's Risk Management Framework process and receives an authorization to operate. Under this process, privacy controls are selected and implemented for this system, and the controls are regularly assessed to ensure that they are effective and operating as intended. One third of all controls are tested each year and the entire system security is reevaluated every three years. The PIA is reviewed and updated on an as needed basis and, at a minimum, every two years.

8.2. Does the system owner continuously monitor and audit the privacy controls to ensure effective implementation?

Yes

8.3. What are the privacy risks associated with this system and how are those risks mitigated?

This PIA details the privacy controls and safeguards implemented for this system in order to mitigate privacy risk. These controls and safeguards work to protect the data from privacy threats and mitigate the risks to the data.

The privacy risk associated with this system is fairly low, as the information collected is not highly sensitive and the information is secured appropriately. Risks to the system include unauthorized access or a user account being compromised. Risk is mitigated by the application and monitoring of privacy controls and by not sharing the information with other systems, third parties, or other users. When a user account becomes compromised, the Department's procedures are adhered to, the user is notified, and the user account is disabled.