Privacy Impact Assessment (PIA)
for the

National Charter Schools Resource Center (NCSRC)
March 11, 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
Contact Email: daryn.hedlund@ed.gov

System Owner

Name/Title: Daryn Hedlund
Principal Office: 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.

The U.S. Department of Education (Department) is required by statute to reserve Charter Schools Program (CSP) funds to conduct national activities in support of the CSP. Under Title IV, Part C, Section 4305(a)(3) of the Elementary and Secondary Education Act of 1965 (ESEA), (20 CFR 4304), the Department reserves CSP funds to (1) disseminate Technical Assistance (TA) both to State entities in awarding CSP subgrants, and to eligible entities and States receiving Facilities Financing Assistance grants, including Grants for Credit Enhancement (CE) for Charter School Facilities and State Charter School Facilities' Financing Assistance Grants (Credit Enhancement Grants) through the CSP; (2) disseminate best practices regarding charter schools; and (3) evaluate the impact of the CSP, including the impact on student achievement.

The National Charter Schools Resource Center (NCSRC) is a website established using CSP funds (https://charterschoolcenter.ed.gov/). It serves as a central location for charter sector resources and publications, upcoming events, relevant news, and funding opportunities. The NCSRC website offers a diverse selection of objective resources on every aspect of the charter school sector for charter school stakeholders and the public. The website also provides an ability for any user to register for a periodic newsletter on charter school-related topics. The website also provides an ability for verified CSP grantees to register for a community of practice, which is a third-party, public website that allows verified grantees, as peers, to exchange grant-related questions with each other and information about the implementation of their grants.

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

Constant Contact (Newsletter)
First name, last name, email address

[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

This information is collected from all persons that wish to receive a newsletter on charter schools related topics. Constant Contact is a third-party servicer that supports the Department by distributing a newsletter using an email list. Individuals may voluntarily sign up for a newsletter that ED sends out periodically with topics central to administering CSP grants.

Groupsite (Third-Party Community of Practice)
First name, last name, email address, and an optional profile photo
This information is collected by Groupsite from only CSP grantees that wish to interact with other verified CSP grantees, as peers, to exchange grant related questions of each other and information about their implementation of their grant. This is a voluntary sign up for a third-party, public website that ED makes available for this purpose of grantee information exchange as it relates to CSP grants. ED only has access to user data that the user makes public in Groupsite. Ed has the ability to remove users and does so when they are no longer a CSP grantee.

Contact Us Form
First name, last name, email address
This information is collected from all users requesting help with the NCSRC website or who have general questions about the charter school sector. The information is only retained until the issue is resolved or a response to the requestor is provided.

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?

New PIA

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 Every Student Succeeds Act (ESSA), Public Law No. 114-95, reauthorized and amended the Elementary and Secondary Education Act of 1965 (ESEA). One of the new provisions, Expanding Opportunity through Quality Charter Schools (referred to in this document as the Charter School Programs or CSP), is authorized under Title IV, Part C of the ESEA, as amended by the ESSA. This provision requires the Department to reserve CSP funds to conduct national activities in support of the CSP. Under Title IV, Part C, Section 4305(a)(3) of the ESEA, the Department reserves CSP funds to (1) disseminate TA, both to State entities in awarding CSP subgrants, and to eligible entities and States receiving Facilities Financing Assistance grants, including Grants for Credit Enhancement for Charter School Facilities and State Charter School Facilities' Credit Enhancement Grants through the CSP; (2) disseminate best practices regarding charter schools; and (3) evaluate the impact of the CSP, including the impact on student achievement.

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.

[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

☑ N/A

The information is not retrieved by name or identifier and is therefore not maintained in a system of records.

Records Management
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 applicable 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.

Constant Contact (Newsletter)
First name, last name, email address
This information is collected from all persons who wish to receive a newsletter on charter schools related topics. This is a voluntary sign up for a newsletter that ED sends out periodically with topics central to administering CSP grants.

Groupsite (Third-Party Community of Practice)
First name, last name, email address, and an optional profile photo
This information is collected by Groupsite from only CSP grantees that wish to interact with other verified CSP grantees, as peers, to exchange grant related questions of each other and information about their implementation of their grant. This is a voluntary sign up for a third-party, public website that ED makes

available for this purpose of grantee information exchange as it relates to CSP grants. ED only has access to user data that the user makes public in Groupsite. ED has the ability to remove users and does so when they are no longer a CSP grantee.

Contact Us Form

First name, last name, email address

This information is collected from all users requesting help with the NCSRC website or who have general questions about the charter school sector. The information is only retained until the issue is resolved or a response to the requestor is provided.

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

Yes

The purpose of the collection is to provide information to individuals who request information from the Department, or to allow interested parties to communicate with each other in a community of practice. The system collects only name and contact information in order to achieve this purpose. To engage with the Community of Practice, users may submit a photo to Groupsite if they wish, but this is not required.

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

For the contact us page, the requesters provide the information directly to the Department through the webpage. For the newsletters, the requesters provide the information to Constant Contact. For the Community of Practice, the requestors provide the information to Groupsite, a third party that hosts the Community of Practice on a non-Department 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.)?

For the contact us information, the information is collected through a webform on the NCSRC webpage. For the newsletters and Community of Practice, the users select a link on the NCSRC webpage, which takes them to a third-party service webpage to provide the information. Constant Contact, the third-party newsletter website, sends the user an email to confirm their request for the newsletter. Groupsite, the third-party

community of practice website, sends ED an email to confirm the user is a CSP grantee. ED confirms and enables the user's account in Groupsite which then sends a welcome email to the user.

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?

For the contact us information, since the requesters provide the information directly, it is likely to be valid. Additionally, the requesters will not receive the information requested or an answer unless they provide the correct information. Constant Contact, the third-party newsletter website, sends the user an email to confirm their request for the newsletter. Groupsite, the third-party community of practice website, sends ED an email to confirm the user is a CSP grantee. ED confirms and enables the user's account in Groupsite which then sends a welcome email to the user. Newsletter and Groupsite subscriber/user accounts are audited by ED's contractor on a routine basis to validate user information. In the case of the newsletter, email addresses that are "undeliverable" are purged from the system. For Groupsite, if the user is no longer a grantee, the account is disabled. Audits of Groupsite users happen weekly, by ED's NCSRC contractor.

Use

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

For the newsletter, email addresses are used to know who has subscribed/unsubscribed. Based on either of these, the user will or will not get the newsletter. Constant Contact collects names of subscribing users in order to address the newsletter to them (e.g. Dear First Name Last Name).

The contact us information is used to provide the information requested.

For the community of practice (Groupsite), the PII (name and email address) is used to authenticate that the user is indeed a grantee by cross-checking it with information on ED's Grant Award Notification (GAN) issued to ED's charter schools grantees.

Initially, an email address is required. Groupsite will verify the email address with the requesting user by sending a verification email to them. Once verified, Groupsite creates an account for the user and asks for first name, last name, and password creation. Then

[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.

the user must respond to two questions: 1) “Is your organization the recipient of a state entity grant from the charter school programs? *this forum is only for CSP state entity grantees. (yes/no)” 2) “Organization Name”. Once entered, an email is generated to NCSRC administrators who validate that the requestor is indeed a grantee before approval to enter the forum is granted..

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.

This PIA provides notice to the public regarding the collection and use of the PII. Additionally, the NCSRC website has a privacy policy.

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://charterschoolcenter.ed.gov/privacy-policy

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?

Requesting funding information or assistance through the contact us form is a one-time collection and use. Users/subscribers to the newsletter can opt out at any time. The user's data is permanently deleted if they opt out of receiving a newsletter or joining the community of practice.

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.

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.

[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.

5.10. 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?

The contact us information is collected for a one-time communication and is not kept. Therefore, there is no information for individuals to access .

For the newsletter, Constant Contact subscribers can unsubscribe at will.

Groupsite users can delete their accounts at will. Users also have the ability to change any information at will.

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

The contact us information is collected for a one-time communication and is not kept. Therefore, there is no information for individuals to access and correct.

For the newsletter, subscribers can unsubscribe at will.

The users/subscribers can update, change, or delete their information on the two third-party service sites, Groupsite and Constant Contact.

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

Contact us information is collected for a one-time communication, so no procedures are necessary.

Users/subscribers are notified on the webpage that they can opt out of receiving emails at any time using the SafeUnsubscribe found at the bottom of every email.

Groupsite has a My Account link at entry and the newsletter has an unsubscribe link in the footer.

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?

Information collected on the NCSRC website is accessible only to authorized users. Physical security of electronic data will be maintained in a secured data center, access to which is controlled by multiple access controls. NCSRC has technical and administrative controls in place that are compliant with the Federal Information Security Modernization Act (FISMA) and with National Institute of Standards and Technology (NIST) standards. NCSRC also operates under an approved Authorization to Operate. When users select a link to go to Groupsite or Constant Contact, the Department provides them with notice that they are leaving the ED environment and are going to the Constant Contact or Groupsite environments. Those environments each have strong security, descriptions of which can be found at the Groupsite webpage and the Constant Contact webpage, respectively.

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.

NCSRC will be authorized for operation in accordance with the Department's Security Authorization Program. As part of the Authority to Operate (ATO) granted by the Security Authorization Program, NCSRC 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 or evaluation include running vulnerability scans and mitigating vulnerabilities within the times specified by the Department in addition to performing yearly self-assessments on one-third of the applicable security controls.

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 NCSRC system owner ensures that the information is used in accordance with stated practices in this PIA through several methods. One method is completing the ED Risk Management Framework process and receiving an Authority to Operate (ATO). Under this process a variety of controls are assessed by an independent assessor to ensure the NCSRC application and the data residing within are appropriately secured and protected. 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. Additionally, privacy risks have been reduced as only names and email addresses are required, and users can personally delete the data or unsubscribe at will. Role-based access controls are implemented to ensure access to data is restricted to authorized users only. System logs record attempted unauthorized access to stored information. User PII will not be posted to the NCSRC website for any reason.

One privacy risk is the unauthorized access, use, or disclosure of PII pertaining to the users. These data breaches involving PII can be hazardous to individuals because they can result in identity theft or financial fraud. The risks are mitigated by the above-mentioned controls and safeguards, updating the security patches and software throughout a continuous monitoring process, limiting access to only those with a legitimate need to know, and working closely with the security and privacy staff at the Department.