Appendix B. Student Roster Collection Request Letter to High Schools

Date

First/Last Name of School Contact
High School Name
Street Address
City, State, Zip Code

Dear (NAME):

Thank you for volunteering your high school to participate in the *Demonstration of Student Messaging in GEAR UP* that the U.S. Department of Education (ED) is funding. This is an exciting opportunity to learn more about whether sending targeted text messages to students can help improve students' college outcomes. At this time, we are asking all participating high schools to provide basic information about their current seniors.

Specifically what we are requesting and why

Students who are currently seniors (in 12th grade) are the focus of the study. In order to know who they are, and to be able to collect information from them, we need a list of the following <u>eight</u> data elements for every senior currently in your school:

1. Name
2. Date of birth
3. Home address
4. Telephone number
5. Student email address
6. Student cell phone number
7. Parent name
8. Parent email address
9. Parent telephone number

Submitting student roster data

We have set up a secure portal that allows you to easily transfer this information to the study team over the web, at a time and in a format that is convenient for you. We expect that compiling and submitting this information will take no more than 2 hours of your time.

By <u>DATE</u> please upload your roster of current high school juniors at:

<div align="center">

http://transfer.abtassoc.com

Your username is: XXXXXX

Your password is: YYYYYYYYY

</div>

Please follow the instructions attached to this email to securely upload your student roster.

Need help or have questions?

A senior researcher from the study team will be contacting you in the next week to answer any questions you may have, and to familiarize you with the portal transfer process.

If you have any questions about participating in the study, you may call 1-XXX-XXX-XXXX, or email me at XXXX@abtassoc.com.

Ensuring confidentiality and data security

ED and its study team, Abt Associates and partners Program and Policy Insight (PPI) and Survey Research Management (SRM), take confidentiality and privacy of information seriously:

1. Under the provisions of the Family Educational Rights and Privacy Act (FERPA), you may disclose this directory information to the study team because they are conducting a federal evaluation on behalf of the Department.

2. All information will be kept confidential at all times. We will follow strict rules to protect the information provided by and about students. Further, we will not provide information that identifies any student to anyone outside the study team and the study collaborators, except as required by law.

3. The secure portal allows you to easily and safely transfer information to the study team over the web. All data will be stored on secure computer networks.

4. All identifying information will be destroyed three years after the study is completed.

Your help is critical to the success of this study and we very much appreciate your involvement!

Sincerely,

Alina Martinez, Ed.D.
Study Project Director

Study Contacts

Alina Martinez	Marsha Silverberg
Project Director	Federal Project Officer
Abt Associates Inc.	IES/US Department of Education
	Marsha.Silverberg@ed.gov
Study Website: www.XXX.com	
Study Email: XXXXX@abtassoc.com	
Study Toll-Free Number: 1-XXX-XXX-XXXX	

Per the policies and procedures required by the Education Sciences Reform Act of 2002, Title I, Part E, Section 183, responses to this data collection will be used only for statistical purposes. The reports prepared for this study will summarize findings across the sample and will not associate responses with a specific program, district, or individual. Any willful disclosure of such information for nonstatistical purposes, except as required by law, is a class E felony.

Paperwork Burden Statement: According to the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless such collection displays a valid OMB control number. The valid OMB control number for this information collection is xxxx-xxxx. Public reporting burden for this collection is estimated to average 2 hours per response, including the time to review instructions, search existing data resources, gather the data needed, and complete and review the information collection. The obligation to respond to this collection is voluntary. If you have comments or concerns regarding the status of your individual submission of this form, application or survey, please contact (National Center for Education Evaluation/Institute of Education Sciences U.S. Department of Education, 555 New Jersey Avenue, SW Room 502i, Washington, DC 20208) directly. (Note: Please do not return the completed instrument, form, application or survey to this address.)

Instructions for Using the Abt Associates Data Transfer Website for the First Time

Please note that any browser can be used but Internet Explorer allows a few additional capabilities. The instructions above are based on the Internet Explorer interface but should be similar enough for Firefox users.

Once you have logged in successfully, you will also have access to an online manual (lower left column) if this guide does not answer all of your questions.

Logging in for the first time

1. 1.   Access the Abt Associates file transfer website by opening a browser and entering the URL:

2. http://transfer.abtassoc.com.

   You will be prompted to accept a certificate. After accepting, enter the username and password included in the email from your site liaison.

   a.   Click the **Sign On** button.

3. You will be prompted to change the password after successfully logging in with the initial password.

   a.   Enter your New Password in the **New Password** field and enter it again in the **New Password Again** field.

   b.   Click the **Change Password** button.

Navigating to your folder

1. From the home screen, type your district/camp/site name into the **Find File/Folder** search box on the left-hand side of the screen.

   a.   Click the **Find File** button.

2. Click on your folder path in the middle of the screen.

3. You are now in your folder.

Uploading a File

1. Under the heading **Upload Files Now…** click on the link (at the bottom) that says **CLICK HERE to Launch the Upload/Download Wizard…**

2. A popup window will appear that is titled **MOVEit Upload Wizard – Upload to…** and has the Abt logo in top left corner.

   a.   Click on the **Add File** button

3. A window will open displaying the files on your computer.

   a.   Navigate to the file(s) you would like to upload, select the file(s), and click the open button. (Note this process is similar to adding an attachment to an email).

      i.   If you have multiple files to upload, hold down the **Ctrl** key while selecting multiple files.

4. Back in the **MOVEit Upload Wizard – Upload to…** popup window, click the **Next** button.

       a. Choose the upload option:

          i. If you only have one file, select *Upload files individually*

          ii. If you have two or more files, select *Upload all files as one .zip*

          iii. Click the **Next** button.

       b. Your file will now upload. The popup window should say *Transfer complete. Integrity verified on all files.*

          i. Click the **OK** button

5. Now back in your folder you should see your file.

6. You should now sign out of the website. The **Sign Out** button is at the top right corner of the screen.

THANK YOU!

Technical Difficulties

IMPORTANT NOTE FOR NON-ABT USERS: The Abt data transfer web portal only accepts connections with TLS 1.0 enabled. Mozilla Firefox and Internet Explorer 7 have this turned on by default. If you are having difficulty even seeing the web site, you probably need to enable TLS. To do so, go to 'Tools -> Internet Options -> Advanced', then scroll down and check the box next to TLS 1.0. Refresh your browser.

The Abt Associates secure data transfer system is based on software that utilizes U.S. and Canadian government validated FIPS 140-2 cryptography. All authentication, data in transit, and data at rest are encrypted.   Furthermore, for security reasons, all data is automatically deleted after 30 days.