

## Guidance for Sharing Student Records with Families During Remote Learning

During remote learning, schools are communicating with families in new ways. As schools continue to connect with families about student progress, it is important that they share information in a secure and confidential manner. This document provides guidance on how schools can securely share information with parents, guardians, and adult students in accordance with [Chancellor's Regulation A-820](#) during remote learning. Specifically, this guidance concerns the privacy of a student's education records. The term "education records" covers any information that is directly related to a student that is being maintained by a school district. It can include an entire document, like a report card. It can also include bits of information about a student found in the student's records, such as the student's grade in a class, their home address, or the name or phone number of their parent/guardian. All such information is considered confidential, and care must be taken when communicating or sharing it.

When sharing education records or information derived from them, schools must make sure that they are communicating with a person who has a right to the information. For students under age 18, this means students' parents or guardians solely. For students age 18 or over, this means the students themselves (also known as "eligible students"). This guidance is accordingly intended as a guide for conducting the following records-related tasks in the context of remote learning:

- fulfilling requests from parents/guardians or eligible students for copies of education records or for information found in those records;<sup>1</sup>
- sending education records to parents/guardians or to eligible students on the school's own initiative (for example, distributing report cards);
- fulfilling requests for education records from third parties (that is, from a party that is neither a parent/guardian, nor an eligible student, nor a DOE employee with a legitimate educational interest in the information), where consent for disclosure has been provided; and
- verifying parents'/guardians' or eligible students' identity when they request changes to student records in DOE source systems, such as ATS or STARS.

This guidance applies to any education record (or information derived from them) that is specific to a student and contains personally identifiable information (PII). Examples of such records include, but are not limited to:

---

<sup>1</sup> In alignment with [Chancellor's Regulation A-820](#), records requests must be fulfilled within a reasonable period of time but not more than 45 days from receipt of the request. Nothing in this guidance document supersedes or replaces [Chancellor's Regulation A-820](#).

- report cards
- transcripts
- verification of enrollment
- authorization for counsel or another third-party to receive records
- NYCSA account creation codes

When sharing education records with parents or eligible students, staff must do the following:

- ensure that they are confident in the identity of the parent/guardian or eligible student with whom they are communicating;
- Make sure that the parent/guardian is not prohibited from receiving education records by checking [Student Profile](#) or ATS; and
- use the instructions provided below for sending encrypted and confidential emails to non-DOE email addresses.

### **Instructions for Verifying Parent/Guardian or Eligible Student Identity**

Schools must always ensure that the adult with whom they are communicating is in fact the parent or guardian or the eligible student, as documented in ATS. Schools should use the [Family Access Management tool](#) or PARD screen in ATS to review all of the adults associated with a student, their relationship, and their level of authorization. Records should only be shared with adults who are parents or guardians or are themselves eligible students. Adults with an authorization code of 07 in ATS have a court order preventing access to that student's records; schools must not share education records or the PII found within them with adults who have this code. For complete information about how to fulfill records requests for various requestors, see question 13 (pages 6-7) of the [student records policy guide](#).

Below are different scenarios schools may encounter when identifying and sharing documents with parents/guardians or eligible students and the steps schools should take in each scenario.

Please note that while non-custodial parents enjoy the same rights to access the records of their children as custodial parents, special rules apply under [Chancellor's Regulation A-820](#). Please see the FAQ below for instructions on how to process requests from non-custodial parents.

#### **SCENARIO 1: The parent/guardian has a full NYCSA account.**

If a requestor is a parent/guardian with a full NYCSA account (i.e., a NYCSA account with their student already attached), schools can securely email student records containing PII using their verified email address. Schools should follow the instructions for sending encrypted and confidential emails with non-DOE email addresses below.

To verify whether a parent/guardian has a full NYCSA account and retrieve their email address, use [Family Access Management](#) (FAM) to begin the process. Navigate to “Student Associations” under Account Management and enter the student’s ID. All adults associated with that student who have a full NYCSA account will appear with their validated email address. If the requestor’s name is listed as a custodial or non-custodial parent/guardian and they have a “Yes” displayed under the column “Access to the Student in NYCS Schools Account,” they are entitled to the student’s records. If the requestor’s name is not listed in FAM for that student as a custodial or non-custodial parent/guardian, this indicates that the requestor might not be entitled to the student’s records because the requestor either (a) has a court order preventing their access to that student’s records or (b) is not associated with the student in ATS. For instructions on using FAM, refer to the [NYCSA FAM Technical Guide](#).

**SCENARIO 2: The parent/guardian does not have a full NYCSA account, but the school has an email address that they’ve been using to correspond with parent/guardian or eligible student, is confident in the parent’s/guardian’s or eligible student’s identity, and can authenticate the parent/guardian or eligible student as the user of that email address.**

Some schools may have collected email addresses from parents/guardians or eligible students that they use with some frequency. As long as the school has previously confirmed that the email address belongs to the parent/guardian or eligible student of record in ATS, the school can securely email the student’s education records using the instructions for sending encrypted and confidential emails with non-DOE email addresses below.

- Once the parent’s/guardian’s identity has been verified, schools should also use the [Family Access Manager tool](#) to create a NYCSA account for the user using one of the following options:
  - In FAM, under “Create Accounts” choose “Online.”
  - In FAM, under “Create Accounts” choose “Authorization Letter-Print Single.” School can email the NYCSA account creation code and instructions to complete the process.

Principals can assign users’ FAM access in Galaxy using these instructions on the [wiki](#).

For detailed instructions, see the [NYCSA FAM Technical Guide](#).

**SCENARIO 3: The parent/guardian does not have a full NYCSA account, and the school does not already have an email address that they’ve been using to correspond with the parent/guardian or eligible student, or the parent/guardian or eligible student contacts the school using a different email address.**

If the school does not have an email for the parent/guardian or eligible student or does not recognize the email the parent/guardian or eligible student is using, the school should take the following steps to verify the identity of the parent/guardian or eligible student by voice or sight. Schools should refer to the [teach from home technology page](#) for instructions on how to use Google Meet or Microsoft Teams.

- If school staff **recognizes** the parent/guardian or eligible student by voice or sight, the school can verify the parent's/guardian's or eligible student's email through phone/teleconference and use this email address to share documents using the instructions for sending encrypted and confidential emails with non-DOE email addresses below.
- If school staff **does not recognize** the parent/guardian or eligible student by voice or sight, the school can take the following steps:
  - Review the photo ID via teleconferencing to verify identity (i.e., name of parent/guardian/eligible student) by matching the name against the student's records found in ATS or [Student Profile](#).
  - If the parent/guardian lacks a photo ID and staff does not recognize the requestor by voice or sight, a school staff member can instead verify the identity of the student by voice or sight. In order to verify the identity of the student, the school staff should have a teleconference with that staff member and student present in the room or the staff member should confidently confirm the student's identity by voice over the phone.
  - If neither of the above options are viable, schools should contact their senior field counsel for further guidance.
- Once the parent's/guardian's or eligible student's identity is verified, the school can request an email address and can securely email the student's education records using the instructions for sending encrypted and confidential emails with non-DOE email addresses below.
- Schools should also use the [Family Access Manager tool](#) to create a NYCSA account for the parent/guardian using one of the following options:
  - In FAM, under "Create Accounts" choose "Online."
  - In FAM, under "Create Accounts" choose "Authorization Letter-Print Single." School can email the NYCSA account creation code and instructions to complete the process.

Principals can assign users FAM access in Galaxy using these instructions on the [wiki](#).

For detailed instructions, see the [NYCSA FAM Technical Guide](#).

### **Face to Face Letters/Proof of Enrollment/Proof of Address**

During this time, when schools are not physically in session, the Human Resources Administration (HRA) will no longer require or ask for "face-to-face" letters as evidence of family composition letters from families who are applying for Cash Assistance (CA) or Supplemental Nutrition Assistance Program (SNAP).

If another agency does require proof of enrollment or proof of address, a parent/guardian can navigate to the "Details" dropdown and take a screenshot of the "Student" page to present as proof that the student lives at the address and a screenshot of "Enrollment" page to present as proof of their student's

current attendance/enrollment. A parent/guardian can follow the same process for proof of student enrollment required for other uses (e.g., for tax purposes). Screenshots should be supplemented by a letter on school letterhead with any additional information the parent requests. For screenshot examples of these pages, please refer to the NYCSA screenshots at the end of this document.

If a parent/guardian does not have a NYCSA account, the school can follow Scenario 2 or Scenario 3 above to authenticate the parent's/guardian's identity.

Once the parent's/guardian's identity has been verified, schools can use [Student Profile](#) to generate both a screenshot of the "Student Details" page to share with the parent/guardian to provide proof of address and a screenshot of the "Enrollment Details" page to show the student is active at their school. Schools should be careful to take screenshots that only include the necessary details that the parents/guardians are requesting. For example, do not include information about Individualized Education Programs, English language proficiency, etc. The school can follow the same process for proof of student enrollment required for other uses (e.g. for tax purposes).

Schools should create an [Intervention LOG \(ILOG\)](#) entry for the student in ATS after sharing proof of enrollment and/or proof of address.

Schools should also use the [Family Access Manager tool](#) to create a NYCSA account for the user using one of the following options:

- In FAM, under "Create Accounts," choose "Online."
- In FAM, under "Create Accounts" choose "Authorization Letter-Print Single". School can email the NYCSA account creation code and instructions to complete the process.

## Frequently Asked Questions

### 1. How should schools respond to requests to update information in DOE systems (e.g., phone number or address)?

Schools must follow the directions described in this document to verify the parent's/guardian's or eligible student's identity and document their request via email. Existing DOE policies apply regarding the documentation required to support a change to the information on student records, including the following:

- Address changes must be accompanied by proof of address. See [Chancellor's Regulation A-101](#) for the ways in which proof of address must be documented. **Schools must not update a student's address in ATS if a family has temporarily relocated.**
- No documentation is required for a parent/guardian or eligible student to change their phone number in ATS. The school should make the requested changes as documented via email. Parents/guardians can also update their cell phone numbers through NYCSA by following [these directions](#).

Additional information about requests to change student biographical information is provided in questions 10-11 (page 5) of the [student records policy guide](#). If schools need additional guidance on how to update student records, they should contact their senior field counsel (general inquiries and legal concerns) or Borough/Citywide Office's academic policy and systems lead (inquiries about academic records and technical support).

**2. How should schools respond to inquiries regarding discharged students?**

Parents/guardians of former DOE students and the students themselves, if over age 18, are entitled to their DOE records. If the requestor has an email address that is already known to and verified by the school, this email address can be used to fulfill the request. If the email address is not familiar, the school should request proof of identify in the form of an image of the requestor's photo ID or using the process identified in Scenario 3 above. Records may be distributed using the directions below for sending encrypted and confidential emails to non-DOE email addresses.

**3. How should schools respond to requests involving third parties (e.g., colleges/universities, employers, attorneys, or other agencies)?**

Third parties can obtain student education records if they submit a valid consent form indicating that they received authorization. A valid consent form must be completed in writing and dated and state the parties or class of parties to whom records may be disclosed, the records or types of records to be disclosed, and the purpose of the disclosure. The consent form must be signed by the parent/guardian (if the student is under age 18) or the eligible student (if the student is age 18 or older).

Parents/guardians or eligible students may consent to the release of records via email provided that schools have followed the directions in this document for verifying the requestor's identity and email address. Schools may use the consent forms provided on pages 15-16 of [Chancellor's Regulation A-101](#) as templates for email consent by having the parent/guardian or eligible student complete the required information and email it back to the school. A physical signature is not required given that the email address has already been verified.

Schools should contact their senior field counsel for additional support.

**4. How should schools manage distributing large quantities of records (e.g., report cards)?**

Schools are encouraged to use existing platforms, including NYCSA, to share academic records such as report cards with families. Schools may also use their existing third-party platforms if already accessible to families. If schools wish to distribute records to large groups of students, they must follow the directions described in this document.

**5. How should requests for education records from non-custodial parents be processed?**

If a non-custodial parent (i.e., the parent with whom the student does not reside) requests access to the student's education records and has access to the student in NYCSA as designated by FAM (see Scenario 1 above), the school can provide the records.

If a non-custodial parent who does not have a full NYCSA account requests access to the student's education records, the school must notify the custodial parent of the request. The notice will tell the custodian of the student that the request has been made, the name of the person making the request, and the date on which the request was received.

The parent making the request shall be notified at the time of the request that the custodial parent is being given an opportunity to inform the school as to whether a legally-binding document or court order specifically revokes the non-custodial parent's rights of access to the records and, if no such document has been produced within 45 calendar days of the receipt of the request, the records must be made available to the non-custodial parent no later than the 45th day. If the custodial parent consents to the release of the records, they may be released as soon as practicable.

Notifications may be made via email but should follow the same authentication procedures as outlined above.

School officials should not provide contact information (including, but not limited to, home address information, telephone or mobile phone numbers, or email addresses) of the custodial parent and student to the non-custodial parent, or to the custodial parent about the non-custodial parent.

## **How to Send Secure Emails through Encryption**

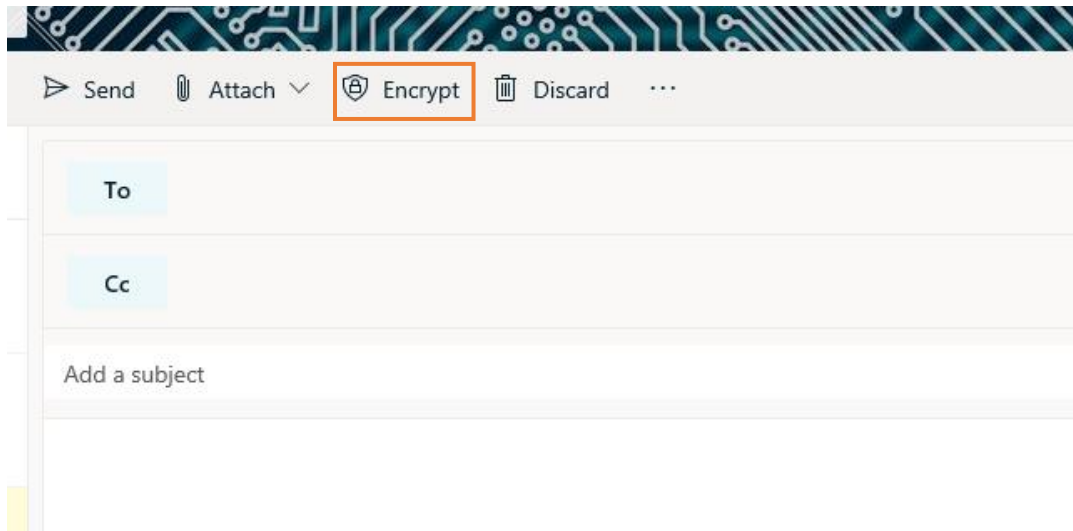
Providing personally identifiable student data to persons who are not authorized to receive such data is unlawful and, in some cases, criminal. Beyond this, it is vitally important that we protect our students from the unintended consequences of their private data falling into the wrong hands. Please use the process outlined below any time an email body or attachment includes PII about a student(s) or DOE employee(s).

Encrypted emails can be sent from desktop computers via the Outlook desktop client, or from any device using the Outlook Web Application. Because the permissions to access an email are saved within the message itself, that access and those restrictions are always enforced—regardless of where the message goes.

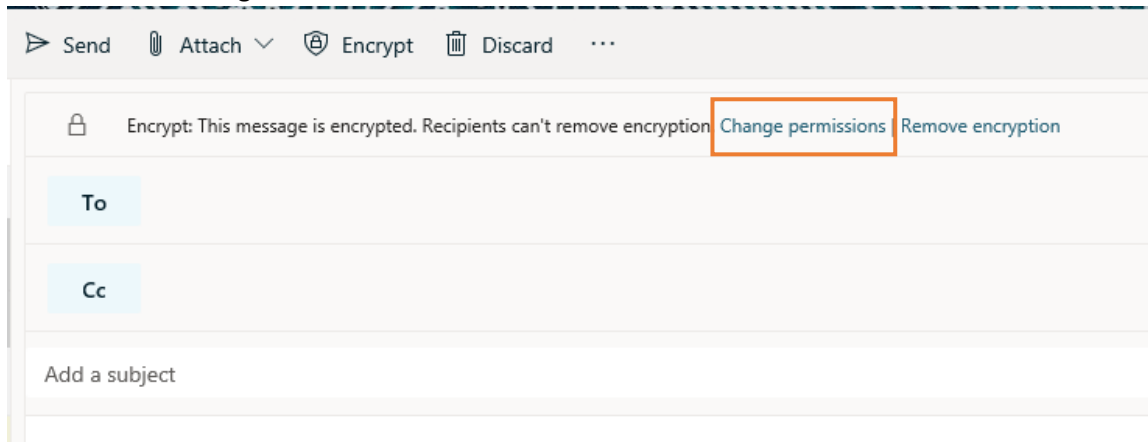
## **How to Set Permissions**

Encrypting an email message in Outlook means it's converted from readable plain text into scrambled cipher text.

1. When creating a new email in Office365/OWA, click the "Encrypt" button.

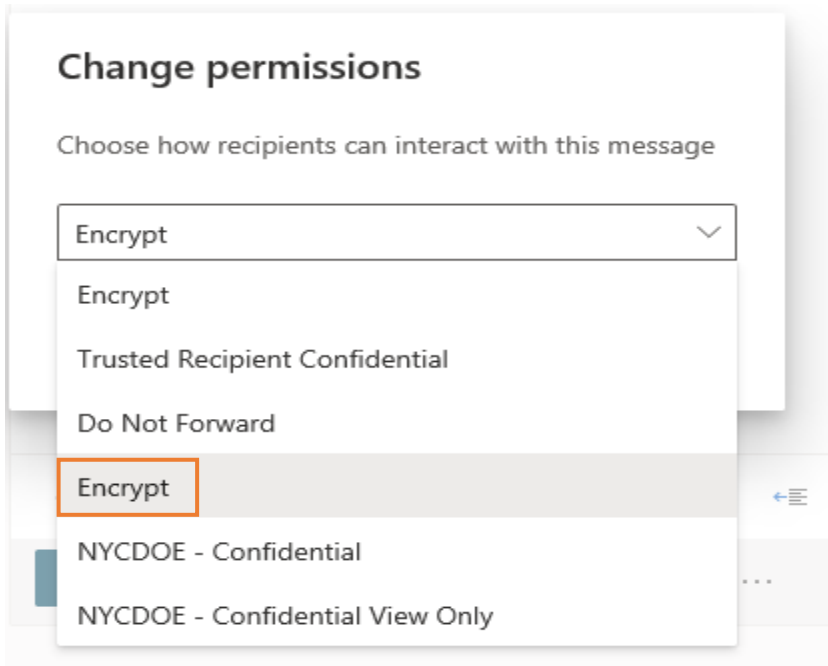


2. Now click on “Change Permissions”



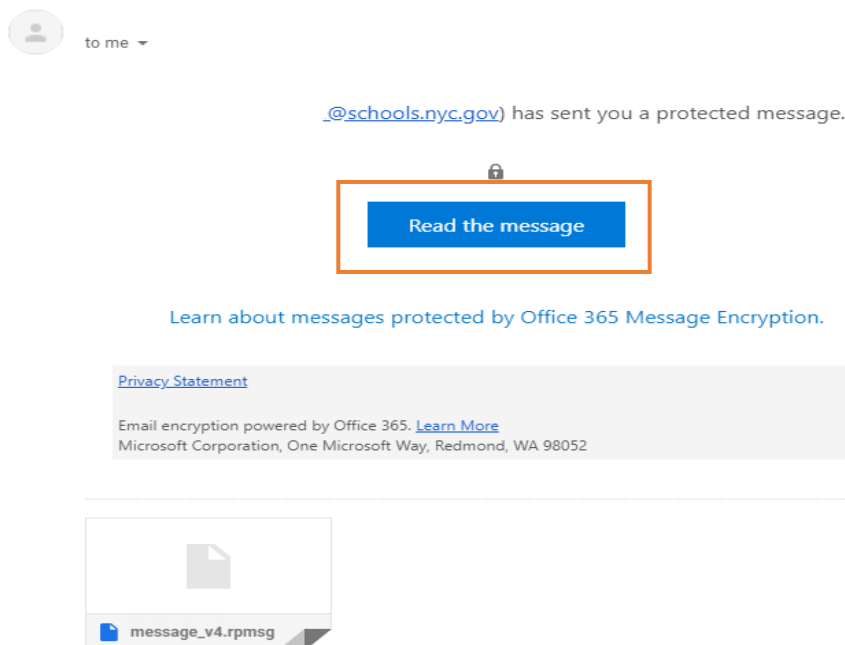
3. You will be presented with various options. Choose Encrypt.





### How to Read an Encrypted Message

1. Recipients will know that access is restricted. The external recipients will receive an email with a link to view the encrypted message. Clicking on “Read the message” will open the message in a browser.

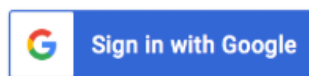


2. Click the “Read the Message” button and then select “Sign in with a one-time passcode”

@schools.nyc.gov has sent you a protected message



Sign in to view the message



Sign in with a One-time passcode

3. Microsoft will send the passcode to the recipient’s mailbox

Here is your one-time passcode

61923791

To view your message, enter the code in the web page where you requested it.

NOTE: This one-time passcode expires 15 minutes after it was requested.

Don't want to use one-time passcode every time you get a protected message? Use your email address to [create a Microsoft account](#)

4. Enter the passcode and click “Continue” to see the message.

We sent a one-time passcode to @gmail.com.

Please check your email, enter the one-time passcode and click continue.  
The one-time passcode will expire in 15 minutes.

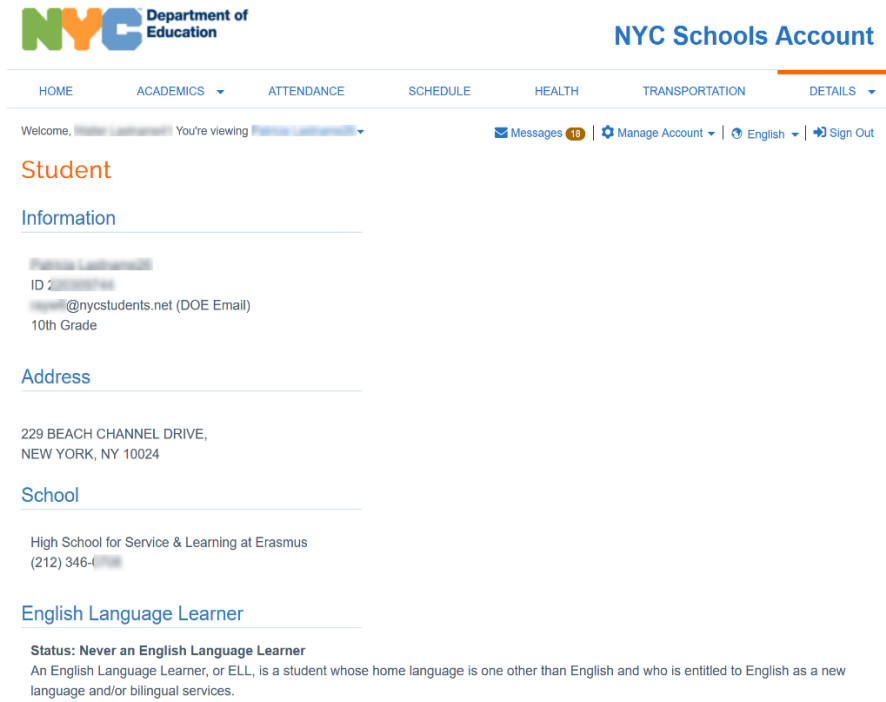
One-time passcode

This is a private computer. Keep me signed in for 12 hours.

Didn't receive the one-time passcode? Check your spam folder or [get another one-time passcode](#).

If the recipient forwards the message, the message will remain encrypted. However, recipients *can* copy the message and paste it into an unencrypted email.

## NYCSA Screenshot Page: Student



**NYC Department of Education** NYC Schools Account

HOME ACADEMICS ATTENDANCE SCHEDULE HEALTH TRANSPORTATION **DETAILS**

Welcome, [Name] You're viewing [Name]

Messages 18 | Manage Account | English | Sign Out

### Student

#### Information

[Name]  
 ID: [ID]  
 [Email]@nycstudents.net (DOE Email)  
 10th Grade

#### Address

229 BEACH CHANNEL DRIVE,  
 NEW YORK, NY 10024

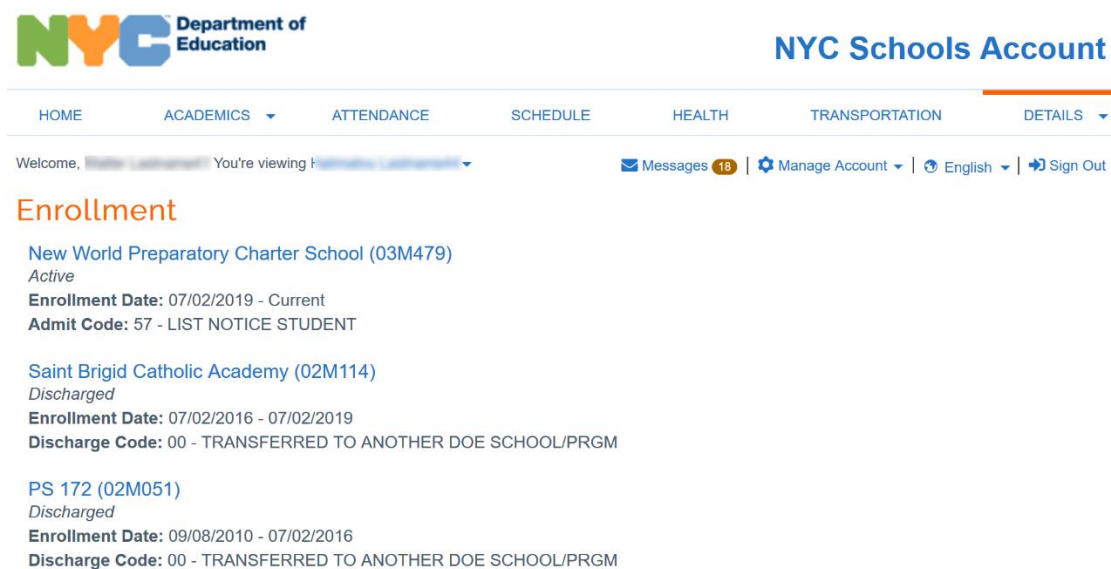
#### School

High School for Service & Learning at Erasmus  
 (212) 346-[Phone]

#### English Language Learner

**Status: Never an English Language Learner**  
 An English Language Learner, or ELL, is a student whose home language is one other than English and who is entitled to English as a new language and/or bilingual services.

## NYCSA Screenshot Page: Enrollment



**NYC Department of Education** NYC Schools Account

HOME ACADEMICS ATTENDANCE SCHEDULE HEALTH TRANSPORTATION **DETAILS**

Welcome, [Name] You're viewing [Name]

Messages 18 | Manage Account | English | Sign Out

### Enrollment

**New World Preparatory Charter School (03M479)**  
*Active*  
**Enrollment Date:** 07/02/2019 - Current  
**Admit Code:** 57 - LIST NOTICE STUDENT

**Saint Brigid Catholic Academy (02M114)**  
*Discharged*  
**Enrollment Date:** 07/02/2016 - 07/02/2019  
**Discharge Code:** 00 - TRANSFERRED TO ANOTHER DOE SCHOOL/PRGM

**PS 172 (02M051)**  
*Discharged*  
**Enrollment Date:** 09/08/2010 - 07/02/2016  
**Discharge Code:** 00 - TRANSFERRED TO ANOTHER DOE SCHOOL/PRGM