

HOW TO REQUEST A SLATE (GRADUATE) ACCOUNT:

Read the policy/guidelines on the use of Slate.

Complete the request form, including a description of your job responsibilities specifically related to the requested access. Select “New User” or “New User-Supervised Access”.

Sign your form, including the Statement of Accountability and submit to College Approver for approval.

Once approved and signed by college approver the User must submit the form via the “[Central Graduate Admissions](#)” SharePoint site.

Confirmation of account creation will come by email.

HOW TO UPDATE/MODIFY A SLATE (GRADUATE) ACCOUNT:

Read the policy/guidelines on the use of Slate.

Complete the request form, including a description of your job responsibilities specifically related to the requested access. Select “Modification”

Sign your form, including the Statement of Accountability and submit to College Approver for approval.

Once approved and signed by college approver the User must submit the form via the “[Central Graduate Admissions](#)” SharePoint site.

Confirmation of account modification will come by email.

HOW TO DEACTIVATE A SLATE (GRADUATE) ACCOUNT:

Whenever an individual is no longer employed or no longer needs access to Slate (Graduate), the user or College Approver should notify the Office of Graduate Admissions.

Complete the request form, including a description of your job responsibilities specifically related to the requested access. Select “Disable”

Submit the form via the “[Central Graduate Admissions](#)” SharePoint site.

POLICY/GUIDELINES ON THE USE OF SLATE (GRADUATE):

You must have a signed Statement of Accountability on file in the Office of Graduate Admissions before you may access Slate for Graduate Programs. Access to certain data/functions may be restricted. Your individual access is based on the level of access assigned to your User ID. You should clarify your level of access within your college. The Office of Graduate Admissions must approve all requests for access.

- Slate records contain confidential, sensitive information and special security precautions must be followed to maintain the integrity and confidentiality of these records.
- Records should only be printed to complete a legitimate business function that cannot be accomplished in Slate (i.e. adding the application record to the department/college student file). Printed documents must be kept in a locked cabinet. Likewise, downloaded documents must be stored on a Georgia State University encrypted computer issued to the user. When you no longer have use of any printed material, please be certain that they are disposed of promptly and properly. Data/exports downloaded from Slate that contain sensitive/confidential information should not be emailed – please use Georgia State’s Send-A-File.
- All endpoint devices must have installed and activated anti-virus, anti-malware and anti-spyware protection software.
- Slate will use the GSU single-sign-on function. For this reason, your User ID is confidential and should only be divulged to authorized personnel.
- Your password should be known only to you. Do not share it with anyone.
- Slate users must enroll in USG’s Duo Multi-Factor-Authentication prior to requesting access to Slate.
- The Slate administrator should be notified of any changes in personnel that affects a User ID, including but not limited to changes in account permissions.
- You must change your password every 120 days or less in accordance to the Georgia State University Information Security policy. The password will expire every 120 days and 2 days prior to expiration, users will be prompted to change their passwords.
- You are accountable for information obtained or changed by your User ID.
- Student Assistants should not be given access to Slate because of the special nature of their employment except when exceptions are authorized for access to non-sensitive non-PII records when supervised access may be granted through a Supervised-Access Account.
- A user should disconnect from his/her ID any time a terminal will be left unattended (break, lunch, etc.), and users should not leave a terminal left unattended with Slate records displayed.
- Monitors should be placed so that unauthorized persons (i.e. students, visitors, unauthorized staff, and anyone else without Slate access) cannot see the screen. This helps prevent an unauthorized party from seeing a person’s record.

- All users having access to Slate should review and be familiar with the University's legal obligation to protect the privacy of student education records under the Family Educational Rights and Privacy Act (FERPA) <https://registrar.gsu.edu/academic-records/records-management/ferpa/> and the university Policy and Confidentiality of Student Information at <https://gsu.policytech.com/dotNet/documents/?docid=204>
- Any questions concerning authorized access and release of applicant information should be referred to the Office of Graduate Admissions.

SLATE (GRADUATE) ACCESS REQUEST FORM

Office of Graduate Admissions

PLEASE PRINT

First Name _____ MI _____ Last Name _____

Check One: New User New User-Supervised Access User Modification Disable

Title _____ College/Department _____

Campus ID _____ GSU Email _____

Roles (Grouped Individual Permissions):

Faculty/Committee Reader | Faculty/Committee Head Reviewer

CEHD:

CEHD Admissions Advisor | CEHD Asst Director | CEHD Dept Staff

RCB:

GRSS Admissions Coord | GRSS Student Services/Experience Staff | GRSS Academic Advisor

GRSS Asst. Dir Admissions | GRSS Director | PhD Asso. Dir | GRSS Recruiter

COTA:

COTA Dept – Grad Coord

All Individual Permissions:

Application Decide | Application Lookup | Application Lookup (Active Period Only)

Application Review Form | Application Update | Deliver

Deliver Send | Deliver Snippet | Events | Form Builder | Interactions | Person Lookup

Person Lookup (Active Only) | Query | Query (Slate Template Library)

Application Sub-Tabs:

International Cred Eval | Decision Process | Waiver (view/update) | AYS Tracking

CEHD Checklist

RCB (view/update)

Restricted Permissions: Must include the specific business-related reason for access to Restricted Permissions.

Database – Letter Templates | Payment Interactions | Person Update

Person Update (Verified Scores) | Test Environment

Please provide rationale for requesting any above restricted permissions:

Graduate Slate Access and Permissions Request Cont.

First Name _____ MI _____ Last Name _____

Please provide a statement outlining the business-related reason you require access to the data.

PLEASE READ THE FOLLOWING STATEMENT OF ACCOUNTABILITY AND SIGN BELOW:

Statement of Accountability

As part of my duties and responsibilities as an employee at Georgia State University, I may be given access to the student/applicant/teaching and learning systems, including PAWS, GoSOLAR, Slate, etc. The privacy of information in these systems is protected by federal and state law and I acknowledge that it is my responsibility to maintain the privacy of those records and to only use the information for authorized purposes related to my work for Georgia State. I have read the guidelines for the use of these systems and understand all of the requirements set forth in those guidelines. I understand that I may not share system passwords with other individuals except as expressly authorized by my supervisor. I understand that employees may not make changes to their own records, even for business purposes, and that making changes known to be false or misleading to any records is grounds for disciplinary action, up to termination. I further acknowledge that my failure to follow the guidelines may subject me to disciplinary action up to and including dismissal as well as possible legal action.

User
Signature: _____

Date: _____

College
Approver: _____

Date: _____

Authorized
Signer: _____

Date: _____

Dir, Graduate Admissions

Permission Descriptions

- **Application Decide**
 - Add, Confirm, Assign Letters, and Release decisions individually from the application record. Also grants access to Decision Management if the user has read access for a query.
- **Application Lookup**
 - Grants read access to view all data on an application tab within the student record.
- **Application Lookup (Active Period Only)**
 - Grants read access to view all data on an application tab within the student record if the application is associated with an active application period.
- **Application Update**
 - Grants write access to application data, including updating the application round, application-scoped fields, submission status, activities, and checklist items.
- **Deliver**
 - Create Deliver messages and edit Deliver messages associated with the user account; Grants access to the Email Gateway Inbox to view emails sent by this user.
- **Deliver Send**
 - Send or stop Deliver messages
- **Deliver Snippets**
 - Create HTML displayable content within Deliver mailings
- **Event Registration (Events)**
 - Create events, access and edit events associated with the user account.
- **Form Builder**
 - Create forms, access and edit forms associated with the user account.
- **Interactions**
 - Grants access to the Timeline tab on the student record.
- **Person Lookup**
 - Grants read access to view a student record.
- **Person Lookup (Active Only)**
 - Grants read access to view a student record that is configured as Active (see the Rules Recipe Book).
- **Query**
 - Create queries and run or edit queries associated with the user account.
- **Query (Slate Template Library)**
 - Grants access to Export and Filter resources in the Slate Template Library while using the Query Builder.
- **Reader**
 - Grants access to the Reader.

- **Head Reviewer**
 - Access to submit admissions decisions in Reader

- **Application Sub Tabs**
 - International Credential Evaluation (View Only)
 - Decision Process (View and Update)
 - Waiver (View and Update)
 - AYS Tracking (View and Update)
 - CEHD Checklist
 - RCB

Restricted/Training Required Permissions

- **Database – Letter Templates**
 - Create and edit decision letter templates

- **Payment Interactions**
 - Create/Update payments on the application record

- **Person Impersonate**
 - Impersonate the contact record - allows updates to application and status page regardless of Application Update Permission

- **Person Update**
 - Grants write access to person data, including updating biographical data, interactions, and person-scoped fields.

- **Person Update (Verified Scores)**
 - Add/update verified test scores

- **Test Environment**
 - Access to test environment