STUDENT-LEVEL DATA REQUEST PROTOCOL (REVISED 9-26-23)

Any request for student-level data must be by **Department Chairs, Directors, or equivalent level**. Faculty and Staff with lower level than Chair or Director should contact your respective department leadership to coordinate data requests. Requestors are responsible for seeking approval from relevant Cal State LA departments/colleges and official(s) prior to IE's review of the request. **Please attempt to use NAVIGATE first (https://www.calstatela.edu/academic/emt/navigate-cal-state-la) for student-level data prior to submitting a request to IE office for student-level data requests.**

All requests must adhere to guidelines set forth by the Family Educational Rights and Privacy Act (FERPA), the University's Institutional Review Board (IRB), and any other relevant university, state or federal guidelines/regulations. You can visit Cal State LA's IRB website at https://www.calstatela.edu/orsca/research-human-subjects-irb .

Please contact IE if you have any additional questions.

PREREQUISITES & REGISTERING WITH MOVEIT

- Registering to MOVEIT: MoveIt is a secure, encrypted file transfer platform, widely adopted across CSU campuses and the Chancellor's Office for transferring files safely. With MoveIt, all files are uploaded and downloaded directly within the secure environment of the site. To ensure the security and privacy of your data, certain prerequisites are required for setting up your login credentials.
- We require users to familiarize themselves with the features and functionalities of MoveIt before initial use. This includes understanding how to upload and download files securely.
- To access MoveIt, visit https://transfer.data.calstate.edu/ . This will lead you to the main page of the MoveIt platform. Before proceeding with accessing the system, please consider the following prerequisites:
  - Ensure that you are either on campus or logged in to the campus Virtual Private Network (VPN). More information about the campus VPN can be found at https://www.calstatela.edu/its/network/vpn .
  - You will also need access to the DUO two-factor authentication app. This adds an extra layer of security to protect your data. If you have not yet installed this app, you can find it at https://www.calstatela.edu/its/2step
  - If you encounter any problems accessing MoveIt via the above link, or if you need help setting up your VPN or DUO two-factor authentication, don't hesitate to reach out to ITS for support. You can contact the Chancellor's Office IT Support Center via email at itsupportcenter@calstate.edu or by phone at 562-951-8500.
- Always verify the recipient before sending files via MoveIt to prevent accidental data leakage.
- See https://csyou.calstate.edu/Tools/IT-Services/ITSupport/Pages/Secure-Data-Transfer-with-MOVEit.aspx for additional information about troubleshooting.

DEPTH AND BREADTH OF STUDENT-LEVEL DATA REQUEST

- Please note that we strive to balance quality data requests with student privacy. This section covers the depth and breadth of student-level data requests and its caveats.
- IE will typically provide the following student-level data when a Department Chair or Director or equivalent person requests:
  - CIN or Student Identification Number
  - Full Name
  - Gender, Ethnicity/Race
- Additional student-level data requests must be reviewed and approved by IE. For example, home address, sexual orientation, military status, etc.
- Four or more identifying information (in total) may not be approved and is typically not supported by IE for valid student-level data requests. This is due to the sensitive nature of the data.

DATA REQUEST PROTOCOL AND SUBMISSION

- When making your data request, kindly indicate whether it is urgent (required within 2 weeks) or non-urgent (needed after more than 2 weeks). This helps us prioritize requests and manage our resources effectively.
- Accompany your request with a list of desired student-level data elements (e.g., CIN, ethnicity, email, etc.). Please arrange this list with the **most critical and relevant information at the top of the list**. We will endeavor to fulfill your

request; however, please be aware that certain items might be excluded due to privacy regulations or legal constraints.

- Please be aware that requests for highly sensitive data often require additional coding and query time to ensure privacy standards are upheld. Such requests are likely to take longer to process due to the extra steps taken in data retrieval, anonymization, or pseudonymization (if necessary). Therefore, when requesting sensitive data, allow for a longer response time to accommodate these necessary measures.
- We encourage you to request only the most pertinent data for your purpose, especially when dealing with sensitive information. This practice aligns with the principle of data minimization, reduces coding time, ensures faster response times, and also upholds better data privacy standards.
- Detail the purpose of your data request. It's essential to state why you need the data and how it will be used. This information allows us to assess the relevance of the request and evaluate any privacy or ethical issues.

DATA HANDLING POST RECEPTION

- Always practice discretion when sharing sensitive data with faculty and staff, after receiving the data. Evaluate the necessity of sharing on a case-by-case basis. Only those who absolutely need the information to carry out their professional duties should have access.
    - Keep all sensitive information encrypted and password protected (update passwords in intervals when necessary). Use strong, unique passwords and regularly update them. Make sure to use a secure method for password storage and sharing.
    - Limit the amount of sensitive information being shared or stored. Wherever possible, use aggregated, anonymized, or truncated data that has had sensitive information removed.
    - Limit physical access to sensitive data. All hard and digital copies of sensitive information should be securely stored and disposed of when no longer required.
- Non-secure channels like email, shared drives, and texting/SMS are typically not as secure and should not be used for transferring sensitive data. Where necessary, use encrypted email or secure file transfer services like MoveIt with robust data protection measures.
- Regularly update and patch all software, including operating systems and applications, to mitigate potential vulnerabilities that could be exploited.
- Carry out regular security training and awareness sessions for your team. This can ensure they are informed about the latest threats and know how to handle sensitive information appropriately.
- Implement a strict privacy policy and ensure it is properly communicated to all staff and faculty. They should understand the potential consequences of violating the policy, including disciplinary action.
- Make use of secure virtual private networks (VPN) when accessing or sending sensitive data remotely.
- Regularly audit and monitor data handling practices to ensure compliance with this protocol.

ADDITIONAL NOTES & FAQ

- Do not share your MoveIt login details with anyone. If you suspect your credentials have been compromised, notify the system administrator (ITS) immediately and change your password.
- Maintain the installed antivirus software and keep your system up-to-date to further secure the data transferred via MoveIt.
- You must be a Department Chair or Director directly involved in the department in which the data request is targeting. For example, a valid data request is if you are the Chair of the Anthropology and requesting student-level data on Anthropology students.
- If you are a Chair of another department, we will need to review your request.
- Be aware of phishing scams. Always verify the source of any unexpected emails related to MoveIt, especially if they ask for your login details or other sensitive information.
- It is essential to ensure that your device is secure and up-to-date before accessing MoveIt. This includes using antivirus software and making sure that all software, including your operating system and web browser, are patched with the latest updates.

Resources:

- https://www.calstatela.edu/provost/college-department-chairs-administrative-coordinators