Student Privacy Frequently Asked Questions

During the 2022-23 academic year, the Graduate and Professional Student Association (GPSA) and Associated Students (AS) conducted a survey of student perceptions of privacy, both at UC San Diego and more generally in society. The respondents posed questions and concerns as part of the survey. GPSA and AS, working with the Campus Privacy Office, have developed this list of FAQs to respond to student questions.

I. General Privacy Questions:

A. Why does privacy matter?

First thing first, privacy isn't just about individual pieces of information or data points about you. Privacy is a broad discipline concerned with our right to make basic decisions about how to live our lives. It is the ability to have control and agency over our bodies, space and personal effects, communications, and digital profiles created with our personal data. It is closely associated with the US Constitutional concept of ordered liberty.

Privacy matters in society for several reasons, including:

- Autonomy and Individuality
- Personal Security and Safety
- Freedoms of Expression, Thought, Inquiry, and Assembly
- Human Dignity and Intimacy
- Trust and Confidentiality
- Innovation and Creativity; Openness in Research
- Democratic Society, Social Movements, and Healthy Markets

Overall, privacy is vital for preserving individual freedoms; fostering personal development, creativity, and innovation; protecting personal information; and maintaining a respectful society. It is a fundamental right that supports human dignity, autonomy, and the ability to lead fulfilling lives. For more, see "In Defense of Privacy."

B. What's data privacy? Why is it important?

Data privacy, a sub-discipline, is concerned with personal data and an individual's digital profile. Information is often collected, combined, and shared by organizations and used to create profiles of individuals consisting of millions of characteristics (data points) about each person. Data brokers and data miners use personal data to create lists such as:

- Impotent persons
- Impulse shoppers
- Likely to tip when presented with a tip screen
- Depressed persons

- Depressive eaters
- Likely last-minute voters
- Likely Alzheimer's patients
- Persons accused of wrongdoing (regardless of actual charging or conviction status)
- Victims of sexual assault

This information is then used for various purposes, such as providing custom services, marketing, nudging, manipulating, or providing (mis)information. To have autonomy over one's own decisions, it is imperative for individuals to be informed about these uses of their digital profiles.

Often, uses of personal data provide substantial benefits to the organization or others, while the risk of harm is borne mostly by the data subjects themselves. Data privacy is, therefore, also concerned with ensuring that uses of personal data provide benefits to the data subjects to the maximum extent practicable in balance with other societal interests.

C. What can individuals do to protect their privacy generally?

Everyone should be mindful about their uses of technology, particularly through social media, websites, and smart devices/IoTs.

A useful goal is to reduce one's digital footprint and curate one's digital profile to the extent possible. Individuals can take several steps to protect their privacy, such as:

- We know that no one wants to read the privacy notices that are associated with the websites and tools we use. However, there is important information in these notices, such as whether you are granting rights to your data for research, whether your data are sold or shared with others, and if your data are used to train algorithms and programs. Carefully reviewing the privacy policies of the services you use, paying particularly close attention to services that sell your information or use personal data to train artificial intelligence (AI) models and algorithms for future use (*e.g.*, text editing services, summarizers, chatbots), is helpful in deciding whether to engage with a website or tool.
- A meaningful practice is to use privacy-protective browsers, search engines, messaging apps, and email services.
- Be cautious about sharing personal information and recognize when metadata and usage and behavioral information about you (such as device IDs, location, engagement behavior, and demographics) are passively collected.
- Reject non-essential cookies (such as marketing cookies) on websites;
- It is great to join loyalty clubs, but it seems like nearly every store has one these days. Ask yourself when you sign up: what are you giving them access to? Do they really need your email and phone number? Your birth date? It is wise to opt out of receiving promotional

materials, discount cards connected to personal data, or participating in marketing surveys if you prefer not to share your data,
- To the extent possible, don't into other sites with your social media identifies (*e.g.*, using Facebook credentials to sign into a website to leave a comment), and not logging out of social media sites before leaving the site.
- Ask services not to sell your data (California requires most businesses to offer a "Do Not Sell My Personal Data" option on their websites/apps).

Note that many websites do not honor "Do Not Track" signals.

These practices are meaningful first steps in protecting your digital profile.

D. How can individuals tell if a service will collect personal information?

Almost every website, application, or service collects some sort of personal information, such as IP address, location, and date and time of access. Many collect additional information about users and combine information from multiple sources to have a broader view of the individual. For example, the car manufacturer Nissan collects information such as sexual activity, health diagnosis data, and genetic information! Individuals should review privacy statements before using online services to ensure they are in line with their expectations. Most organizations also have a privacy office that can provide more information and access to one's own data. For more, see the Mozilla Foundation's Annual Consumer Creep-o-Meter. (https://foundation.mozilla.org/en/blog/state-of-online-privacy-reaches-very-creepy-level-finds-mozillas-first-annual-consumer-creep-o-meter/)

E. Are there educational materials available for those interested in learning more about privacy?

Yes! The Campus Privacy Office provides training, education, and awareness services. The flagship educational course Privacy 101 Workshop is available to the public at no cost. It is recommended for those interested in the history, discipline, and importance of privacy and data ethics, with particular attention to modern data practices and their impacts on current events, society, and personhood. Beyond data privacy, learners will develop a deeper understanding of bodily/intimacy privacy, territorial privacy, communication privacy, and surveillance capitalism.

UC San Diego affiliates can learn about UC San Diego specific requirements through the following on-demand courses in UC Learning:
- Confidentiality of Student Records and Privacy Rights – FERPA
- Privacy @ UCSD

A list of educational offerings can be viewed from the Campus Privacy Office website: https://privacy.ucsd.edu/

II. Questions about UC San Diego's Personal Data Practices:

A. What kind of data does UC San Diego collect about applicants and students?

UC San Diego collects various types of data about applicants and students, including personal information like names, addresses, dates of birth, Social Security Numbers, and information about parents/legal guardians. The university also collects or creates academic data such as grades, transcripts, course registrations, attendance records, and progress towards degree completion. Additionally, UC San Diego may gather information related to student activities and needs, financial aid, student health, disability information, military affiliation, and participation in campus events or programs. As with most organizations, the University also maintains logs of metadata (*e.g.*, device info, location, date and time of access) related to student uses of IT resources, such as the University website, app, and learning management software (Canvas).

B. How does UC San Diego use the data it collects about students?

UC San Diego uses the collected data for a variety of purposes related to education, administration, and support. These include:

- Managing academic programs and records,
- Facilitating enrollment and course registration,
- Providing financial aid services,
- Improving services and security,
- Supporting student health, well-being, and safety,
- Supporting campus activities and programs,
- Conducting research to enhance educational experiences and to study trends in student performance or to improve teaching methods,
- Complying with legal and regulatory requirements,
- Conducting surveys and providing information that may be of interest to students, such as scholarship or employment opportunities, and
- For alumni and advancement purposes.

C. Are student data protected by privacy laws?

Yes, student data are protected by several privacy laws, including the Family Educational Rights and Privacy Act (FERPA), California Information Practices Act (IPA), the Gramm-Leach Bliley Act (GLBA), and, in some circumstances, by the European Union's General Data Protection Regulation (GDPR). These laws require universities to obtain consent from students in many cases before sharing their data with third parties and to take steps to ensure that the data are secure and protected from unauthorized access and use. Students can review the UC San Diego Notification of FERPA Rights here: https://students.ucsd.edu/sponsor/registrar/ferpa.html

UC San Diego also complies with UC privacy policies, such as those related to student information, health information, cybersecurity, and law enforcement. A list of all UC policies that have privacy aspects can be found here: https://www.ucop.edu/ethics-compliance-audit-services/compliance/privacy/privacy-policies-and-references.html

UC San Diego takes measures to ensure the security of student data, restrict access to authorized personnel, and employ appropriate technical safeguards to mitigate data breaches and unauthorized access. In addition to legal compliance, UC San Diego has developed its Privacy Guiding Principles, which apply to all personal data.

D. Does UC San Diego share student data with third parties?

UC San Diego may share student data with authorized third parties under specific circumstances. This can include sharing data with government agencies as required by law, sharing information with other educational institutions for academic purposes (such as study abroad programs or credit transfers), or sharing data with vendors or service providers contracted by UC San Diego to deliver certain services (*e.g.*, technology platforms, financial aid disbursement).

When sharing sensitive data with service providers (*e.g.*, Canvas, Piazza, GradeScope), UC San Diego must review them and makes sure that contractual requirements are in place to protect student data from unauthorized or inappropriate uses or disclosures, including for marketing purposes.

E. What about enterprise software such as Google G-Suite, Microsoft OneDrive, and Zoom?

Same as above, all enterprise software purchases go through security review. There are contracts in place to ensure these programs comply with UC information security requirements, as outlined in the UC BSF-IS-3 Policy.

F. Can students access and control their own data?

Yes, students have the right to access and review their own records held by the university, as required by FERPA. Students can do this through the university's student portal or by submitting a formal request to the Registrar's Office or through Policy and Records Administration, which administers Information Practices Act requests. Students also have the ability to update or correct their data if they are found to be inaccurate or incomplete. However, some restrictions may apply to certain types of data, such as confidential health records, grades, or third-party information shared under limited conditions.

The European Union also gives certain data subject rights to covered individuals in the EU. To exercise EU GDPR data subject rights, individuals can complete the Data Subject Request To Restrict, Object To, Or Delete Personal Data. UC San Diego will do its best to address requests. However, it will not be able to

delete information that it is otherwise required by law or UC Policy to maintain. UC San Diego will also not be able to honor requests to delete official academic or employment records.

G. Does UC San Diego monitor student emails, internet use, or application use on the university network?

No. The UC Electronic Communications Policy (ECP) and UC San Diego PPM 135-5 place stringent limits on when and how the university can access electronic communications, including internet searches. Per the ECP, the University can examine electronic records without the consent of the holder only: (i) when required by and consistent with law; (ii) when there is a substantiated reason (as defined) to believe that violations of law or of certain University policies have taken place; (iii) when there are compelling circumstances (as defined); or (iv) under time-dependent, critical operational circumstances (as defined). In addition, as with most organizations, the university uses automated means to monitor internet traffic for suspicious activity and security threats.

H. What access, if any, does the UC San Diego campus administration have to student medical records?

None. Student health records, which are covered by FERPA, are stored in the UC San Diego Health Epic electronic health record system. This information is firewalled and protected at the same level as any other patient record that is subject to HIPAA. When there are legal requirements, such as OSHA/CDPH requirements for universities to report positive COVID results, UC San Diego Health will provide pertinent, required information – and only the minimum necessary information -- to campus upon request. However, campus officials do not have any access to student medical records and may not request information that is not legally required or permitted.

I. How can students learn more about how UC San Diego handles personal data?

Students should first review UC's privacy policies and guidelines available on the university website. If further assistance is needed, students can contact the UC San Diego Campus Privacy Office for campus practices and the UCSD Health Office of Compliance and Privacy for questions related to Student Health records. Students should report any suspected data breaches or unauthorized access promptly to ensure appropriate action can be taken.

J. Who can answer privacy questions and address concerns?

The UC San Diego Health Office of Compliance and Privacy can answer questions related to student health as well as privacy practices at UCSD Health and UCSD Health Sciences. The website is here: https://medschool.ucsd.edu/compliance/privacy/Pages/default.aspx

For all other privacy concerns, including for campus, SIO, Preuss School, Extended Studies, and SDSC, the Campus Privacy Office can provide assistance. The website is here: https://privacy.ucsd.edu/ The Campus Privacy Office offers the following services to the campus community:

- Governance
- Policy and principles development; policy analysis
- Campus privacy balancing process and framework (with the ISPC)
- Training and awareness
- Vendor/collaborator assessments and selection
- Consent documents and privacy notices
- Contract negotiations
- Data subject requests
- Advocacy
- Research
- Documentation of processes and data lifecycle inventories
- Privacy incident mitigation, investigation, and notification