Consortium of Universities of the Washington Metropolitan Area
Privacy Policies

Principles and Practices

The Consortium is a nonprofit educational association of 17 member colleges and universities representing nearly 290,000 students committed to the advancement of higher education in the Washington Metropolitan Area. To serve students, the Consortium manages the student cross-registration program, the Consortium Research Fellows Program, the U.S. Institute of Peace program, Reach4Success, and the Campus Public Safety Institute. See the separate tabs on these topics for more information. The Consortium brings together numerous campus groups several times each year, including the emergency managers, chief academic officers, chief financial officers, chief student affairs officers, health center directors, government relations staff, public relations staff, admissions and financial aid staff, registrars, and others as the need arises. The Consortium provides a unified voice on behalf of its members to local and regional governments, as well as to business/industry and other organizations by serving as a single point of contact, by participating on boards and as members of organizations, and through convenings. The Consortium provides numerous services to its members, including government relations and organizational liaison functions, and joint responses to various opportunities (e.g., RFPs, grants, collaborative projects). Above all, Consortium institutions focus on three overarching goals: creating an educated populace; creating and promoting a dynamic, innovative atmosphere; and creating the future economy.

Given these activities and goals, all who are part of the Consortium—staff, institutional members and their representatives, student interns and research fellows, faculty fellows, and third-party contractual organizations—have an obligation and responsibility to respect the privacy rights of individuals. Consequently, the Consortium strives to incorporate privacy practices into the design of all of its systems and processes based on “privacy by design” principles. This is put into practice through our commitment to define,
Consortium Privacy Policy
Page 2 of 9

communicate, and enact privacy policies and procedures consistent with the following standards for any information collected:¹

1. **Notice and Awareness.** The Consortium provides notice to individuals related to privacy policies and procedures, explaining the purpose for which the personal information² is collected, used, retained, and disclosed. The privacy notice is visible, readily accessible, and dated to allow individuals to determine if the notice has changed. *The Consortium respects and wants to protect your privacy and intellectual property. There is no secret data collection.*

2. **Choice and Consent.** The Consortium acknowledges that each individual exercises choice about how visible they wish to be. Therefore, choice is provided to the individual, including which personal information is initially collected and how and under what circumstances this information is provided to third parties. In the case of employment and payroll records, the specific data required to be collected and retained for verification of enrollment in an academic program or of employment and payroll will be explained. Information is used and retained for specific internal Consortium purposes and is not used for other purposes without appropriate notification or authorization. Specific enrollment- or employment-related information that is required to be shared with contracting organizations by law or regulations for purposes of permitting the individual to conduct their studies or work at those locations will be explained. The Consortium will make reasonable efforts to keep services as open as possible, and will inform individuals of the limitations of service that may result from their choices. *Users have a choice on whether or not to provide personal information not required by law or regulations.*

3. **Clear Usage, Retention, and Disposal Practices.** The Consortium’s use of personal information is limited to the purposes identified in the description of the service or process for which the individual has provided implicit or explicit consent. To the extent it occurs, personal information is collected in a manner that preserves the privacy of the individual and is retained for only as long as necessary or as required by law or regulations to fulfill the stated purposes. Such information is thereafter appropriately destroyed or discarded. If a person declines to provide required personal information, the Consortium may be unable to provide a service,

---

¹ These privacy principles are based on widely used U.S. federal Trade Commissions’ five Fair Information Practices and Principles (FIPP): transparency, choice, information review and correction, information protection, and accountability. The Consortium has also reviewed the European Union general Data Protection Regulation (GDPR) standards regarding privacy notices, the concept of consent, data stored in the cloud, and security breach notification.

² Personally identifiable information, as used in U.S. privacy law and information security, is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.
employment, or employment verification. The Consortium only collects the data needed, and only uses it as stated.

4. Access to Information. Access to information is limited to those with direct and expressed authorization to have access for those purposes for which the information was provided. The Consortium will periodically inform individuals about pertinent personal information being held and will provide the individual with means for review and update. The Consortium will never sell private information to third-party vendors, and will be clear about third-party website or transactional interactions where applicable, and how they are governed. Individuals have the right to review and correct personal information.

5. Integrity and Security for Privacy and Accountability Processes. The Consortium has the responsibility to protect private information, and will provide administrative, technical, and physical safeguards of the information, including periodic quality assessments and notification in the event of a security breach. The Consortium assumes the responsibility to protect the quality and security of information collected.

Master Privacy Policy

The Consortium is committed to protecting your privacy and we honor your right to make choices about the information you share. This Privacy Policy describes how the Consortium collects information, including certain personally identifiable information, and how the Consortium may use, process, and share such information.

The Consortium retains the right to change this Privacy Policy at any time, but will notify you of significant policy changes. Individuals should review the Privacy Policy regularly to learn about other changes. Your use of the Consortium website(s), including any apps, constitutes your acceptance of the Privacy Policy, including periodic changes.

Consortium services and benefits are not designed or intended for minors, and we do not knowingly attempt to solicit or receive any information from minors. To the extent that minors under the age of 13 do use a Consortium website or app, and the Consortium is able to determine the age of the user(s) through their submissions to or communications with Consortium websites or apps, the Consortium will not knowingly collect information from such minors without their parent’s or guardian’s verifiable consent.

Every Consortium staff member, contractual organization, and individual who has access to data or personal information collected by the Consortium is charged with respecting the
privacy of those who provided it and is expected to respect and follow the Consortium Privacy Policy.

Collection and Use of Information

To fulfill its mission and goals, the Consortium collects information about those who are employed or work under the auspices of the Consortium, or are students in the various academic programs and professional development and employee training programs and about those who engage with us via email and/or visit our website(s) and access our apps. This information and the data derived or collected are used, in part, to improve the communication about the Consortium’s activities, to improve our programs, websites, and apps, and to serve the interests of our members through services, employment/payroll, and/or employment verification.

Through your interaction with the Consortium, you may be asked for personal information such as name, mailing address, phone, email address, or other personal information so that we may provide the service requested or respond to your information request. If you are employed at the Consortium or in any of the Consortium’s subsidiary programs, additional information regarding required by law or regulations for employment verification and payroll will be collected. If you are registering through the cross-registration program or for employment-related training, information regarding the course(s) or program(s) for which you are registering, along with supporting academic information, will be collected. If we are requesting that you provide this information in an email attachment, you will be asked for your consent to do so. As described later in this Privacy Policy, a decision to not provide required personal information may result in the Consortium not being able to provide the service, employment/payroll, or employment verification requested.

Once collected, the Consortium may use this information in a variety of ways, which may include:

- Communication with you about your inquiry, academic or employment training registration, or to communicate information about the Consortium.
- Providing prompt and effective customer service.
- Building higher quality and more useful services, such as by analyzing usage trends and interests regarding specific websites and apps.
- Conducting internal assessments of Consortium programs.

Consortium institutional members may add, correct, or update their information by sending the update to info@consortium.org. Employees and students may request to review or update information by following the process described in the subsequent section entitled “Access to and Ability to Correct Data.”
Sharing with Third Parties

The Consortium does not sell or rent postal or email lists. The Consortium will occasionally mail or email a notice or survey on behalf of another organization to selected individuals at member institutions and others who may have interest in receiving the notice or survey, when such material is deemed to be beneficial to those being contacted. Such mailings and emails are subject to the review of Consortium staff and board members, depending upon the nature of the message.

The Consortium reserves the right to disclose information, including personal information obtained through its websites and apps, when disclosure is required by law, regulations, or in a good-faith belief that such action is necessary to: (a) conform to legal requirements or regulations, or comply with legal processes served on the consortium; (b) protect or defend the rights or property of the Consortium; or (c) protect the personal safety of Consortium officers, staff, students, contractual organizations, or members of the public in appropriate circumstances.

Opt In/Opt Out

The Consortium reserves the right to offer either an opt in or an opt out option depending on the situation and the type of information being collected. Any individual may decline to provide information requested by the Consortium. In this case, the Consortium may be unable to provide services or employment for which such information is needed for security and/or identity purposes.

Access to and Ability to Correct Data

Upon request via postal mail, email, telephone, or voicemail, the Consortium will respond to an inquiry from an individual regarding their right to review and correct personal data. Once a request has been received, the Consortium will contact the individual making the request and require identity verification prior to providing the individual with a summary of any personally identifiable information retained by the Consortium regarding the individual making the request. Individuals may then modify, correct, change, or update personally identifiable information that the Consortium has collected through its website(s), apps, or other means (including, but not limited to paper forms) and/or may initiate the removal of their personal record from the Consortium’s database by contacting Erin Pate at the Consortium by phone at +1-202-331-8080 x110 or by email at epate@consortium.org. As noted, identity verification will be required for this process to occur. Individuals are reminded that removal of information required by law or regulations
may be impermissible or may result in the Consortium being unable to provide services, employment/payroll, and/or employment verification. Questions about this process may be submitted by email to info@consortium.org.

**Keeping Data about Individuals Secure**

Personal data are stored on a secure server, in locked filing cabinets, or in a secure offsite location. Procedures have been employed at the Consortium and through our information technology partners to safeguard the security and integrity of your information. Although the Consortium takes these measures to safeguard against unauthorized disclosure of a person’s data or personal information, the Consortium cannot control internet transmissions and cannot guarantee or warrant that data or personal information transmitted to the Consortium will be uncompromised in all circumstances.

**Data Retention**

The Consortium follows all federal, state, and local laws and regulations regarding data retention. In situations not covered by federal, state, or local law or regulations, if historical activity pertaining to Consortium business needs is present, the information may be kept indefinitely. Individuals may request an anonymization of their record by contacting Erin Pate at the Consortium by phone at +1-202-331-8080 x110 or by email at epate@consortium.org. Identity verification will be required for this process to occur. Individuals are reminded that anonymization of information required by law or regulations may result in the Consortium being unable to provide services or employment/payroll and employment verification.

**Cookies and Other Technologies**

A “cookie” is a file that a website stores in a user’s computer for future reference. Individuals may set their browsers to reject cookies. Information supplied through a Consortium cookie is used only by the Consortium to help enhance services provided and is not shared with others.

Web “beacons” are transparent pixel images embedded at certain points on websites that are used to collect information about how users navigate and use the website for the purpose of understanding and improving the function of the site and the value of the content. The Consortium uses cookies and other trackers to improve its services, provide enhanced functionality on the website(s), and to aggregate traffic data (e.g., what pages are the most popular).
Cookies and beacons may also be utilized by the third parties we contract with to provide certain functions. You may block or disable cookies and other trackers by changing the settings on your browser, but doing so may prevent you from accessing certain functionalities or impair your experience in interacting with the website(s).

**Commitment to GDPR Compliance**

The Consortium is committed to complying with the terms and spirit of the General Data Protection Regulation (GDPR), the comprehensive European Union data privacy law effective May 25, 2018. We are committed to communicating the steps the Consortium is taking to ensure GDPR compliance.

The GDPR’s requirements have many implications, and the Consortium is conscientiously working to ensure that our services and contractual commitments are brought into compliance. Among the measures the Consortium is taking are:

- Reviewing vendors and contracts to ensure that the appropriate measures are in place, and updating contracts as needed;
- Auditing lists (e.g., email distribution lists) to determine how consent was granted and taking appropriate steps accordingly;
- Ensuring we can support international data transfers and communications;
- Employing privacy tools and utilities for data portability and management; and
- Continuing to invest in our security infrastructure and practices.

The Consortium will continue to monitor the guidance regarding GDPR compliance from privacy-related regulatory bodies and will adjust our practices accordingly to implement any changes or interpretations to the regulation and will continue to make updates to this Privacy Policy.

**Third Party Websites and Services**

The Consortium links to other websites that are not controlled by or contracted to the Consortium. A link from the Consortium website is not an endorsement of any company, organization, individual, or viewpoint. The Consortium is not responsible for the privacy practices or the content of those sites. The Consortium also contracts with third party service providers for information technology services and transactional services. In those cases, the Consortium will strive to ensure that third party privacy practices are aligned with and abide by the Consortium Privacy Principles Privacy Policy. You should review third party privacy policies in connection with visiting other websites.
Intellectual Property Rights and Protection vs. Personal Privacy

Protection of intellectual property is the responsibility of individuals. The Consortium has policies and practices in place to help support this protection. Violation of intellectual property rights are legally covered through intellectual property laws, not privacy laws. Likewise, the Consortium Ethics Policy rather than the Consortium Privacy Policy is applicable for intellectual property concerns. Individuals are asked to contact the legal officers at your home institution, company, or organization if you believe you have experienced an intellectual property violation related to Consortium programs or services.

Changes to Policy

The Consortium reserves the right, at any time, to add to, change, update, or modify the Privacy Policy simply by posting such addition, change, update, or modification online on its website. Any such addition, change, update, or modification will be effective immediately upon posting on the website. When significant changes are made to the Privacy Policy that will directly impact how personal data are collected or used, the Consortium will notify you by additional means, such as posting a notice on the website or some other mechanism. Users should review the Privacy Policy regularly to learn about other changes.

Governing Law

By choosing to visit our website(s) or apps, or provide information to us, you agree that any dispute over privacy or the terms contained in this Privacy Policy will be governed by the laws of the District of Columbia and the United States of America. The Consortium makes no representation that this Privacy Policy and such practices comply with the laws of any other state or country. Visitors who use the website(s) and apps and reside outside the United States do so on their own initiative and are responsible for compliance with local laws, if and to the extent local laws are applicable. If you reside outside the United States, by using the website(s) and apps, you consent to the transfer and use of your information outside your country. These data transfers are necessary to provide you services as a user of the website(s) and apps.

Questions Regarding the Privacy Policy

If you have questions about our Privacy Policy or Privacy Principles, or use of this website in general, please contact us by email at: info@consortium.org.