DATA PROTECTION POLICY

Responsible Office: Office of Privacy
Date Created: 12-07-2021
Date Approved: 11-10-2021
Next Update: Annually from date of issue

Webster University, Office of Privacy

DATA PROTECTION POLICY

1.0 Purpose

Webster University (the University), is committed to protecting the privacy and security of the personal data it processes on behalf of its students, applicants, alumni, employees, faculty, and the wide range of other constituents it works with as an academic institution, employer, and partner. In order to do this, the University commits that:

- We process all personal data fairly and lawfully.
- We support the rights of individuals.
- We keep our personal data secure.
- We design privacy into our systems and processes.

Like all educational establishments, the University holds and processes personal data for a variety of purposes including, for example, administration of the admissions process, recording academic progress, providing welfare services, operating payroll, and enabling correspondence and communications.

2.0 Scope

The University is subject to the EU General Data Protection Regulation (EU/2016/679) (GDPR or the Regulation) and the national data protection legislation in force in the countries in which it operates. Under the GDPR legislation, the University is classified as a data controller.

3.0 Definitions

The GDPR governs the processing of personal data. The following definitions are used:

Personal Data is data which can identify living individuals. As well as images, names, and contact details, it can also include numerical or statistical information from which an individual's identity can be derived.

Special Category Data is personal data revealing physical or mental health, disability, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data capable of uniquely identifying a natural person, and data concerning a person's sexual orientation.

Data Subject is the individual who is the subject of personal data. Data subject is always a human individual and not an entity or corporation.

Data Controller determines the purposes for and the means by which personal data is processed. The controller is ultimately responsible for the personal data, why the data is processed and who it is shared with, including responsibilities for ensuring the rights of individuals over the processing of their personal data are upheld.

Data Processor is any individual or organization who processes personal data on behalf of the data controller.

4.0 Principles

The University is required to process personal data according to the following principles:

Data Protection Principles	The context for the University
Lawfulness, fairness, and transparency	The University explains to its employees, students, and other constituents how and why it processes personal data at the point of collection.
Purpose limitation	The University only uses the personal data for the reasons it was collected.
Data minimization	The University only collects the minimum amount of personal data necessary for the purposes it is collected.
Accuracy	The University ensures that the data is correct, up to date and it is able to rectify any inaccuracies or mistakes quickly.
Storage limitation	The University does not retain personal data for longer than it is needed.
Integrity and confidentiality	The University protects its personal data against unauthorized access, loss or destruction by implementing a range of technical and organizational security measures.
Accountability	The University is able to demonstrate that it meets its obligations for compliance.

5.0 Lawful Basis for Processing

The University needs to meet one of the six lawful bases in order to process personal data. The most common for the University will be the following:

Lawful Basis	Examples for the University
Necessary for the performance of a contract or service to which the individual is a party.	Covers the majority of processing for its employees and faculty.
Data subject has given consent to the processing.	Covers Alumni activities, mailing lists, marketing and other 'opt-in' services for students and other constituents.
Necessary for the purposes of the legitimate interests pursued by the University or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject.	Covers activities relating to charitable works, fundraising and donations, Alumni, research, honorary degrees and ethical donations.

6.0 Lawful Basis for Processing – Special Category Data

For special category data, in addition to the lawful bases listed in Section 5, the University is required to have an additional lawful basis for processing special category (sensitive) personal data, as set out in Article 9 of the Regulation.

Legal Basis	Examples for the University
Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment, social security, and social protection law.	Sickness absence, workers council/union membership.
Processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee.	Fit to work assessments, health and safety assessments.
Processing is necessary for archiving purposes in the public interest, scientific or historical research or statistical purposes.	Analysis and reporting of equality and diversity information.
Criminal or alleged offences.	Exemptions for the purposes of prevention or detection of crime reporting to law enforcement bodies.

The lawful basis for processing personal data will be listed in the University's Record of Processing Activities (ROPA) produced in line with Article 30 of the Regulation.

7.0 Rights

Data Subjects: All individuals whose personal data is processed by the University, have a number of rights under the Regulation. These include:

Right	The Context for the University

A fundamental right to be informed about the processing of their personal data and who to contact if they have any questions, concerns, or complaints about that processing.	Data subjects have the right to be informed about the purposes of the University's processing of their personal data before it is collected. The University provides this information via the publication of its Privacy Notices for prospective, current and former students, alumni and friends of the University and faculty, and for prospective, current and former employees.
A fundamental right to have personal data processed securely.	The University provides technical and organizational measures to protect the processing of its personal data. Those security measures are applied in relation to an assessment of risks (see Section 9.0).
Right of access	Data subjects have the right to be informed about what the University is doing with their data, check that it is held and used correctly, and obtain a copy.
Right to rectification	The University makes every effort to ensure its data is accurate. If a data subject believes some of the data the University holds about them is inaccurate, they can ask for this information to be corrected. The Office of Privacy will assess the request and respond accordingly.
Right to erasure	Data subjects have the right, in limited circumstances, to ask the University to remove or delete data it holds about them. The Office of Privacy will assess such requests and respond accordingly.
Right to restrict processing	Data subjects may, in the course of a dispute with the University regarding the use of their personal data, ask the University to stop using their data if certain criteria apply.
Right to data portability	Data subjects have the right to ask the University to provide them with a re-usable electronic copy of their data to allow them to transfer it to another controller. This only covers data submitted to the University by the data subject or data observed from the data subject's use of a service, if technically possible. The University may

	consider transferring electronic information directly to another data controller requested by the data subject.
Right to object	Data subjects have the right to object to processing based on legitimate interests, legal obligation, for the purposes of direct marketing or for "scientific or historical research purposes or statistical purposes". The Office of Privacy will assess such requests and respond accordingly.
Automated decision making, including profiling	If the University is making decisions about a data subject solely through automated means, such as a computer algorithm, data subjects can appeal against the decision. The Office of Privacy will ensure that data subjects can express their point of view and enable a review and explanation of the decision.

None of the above rights is absolute. Anyone who wishes to exercise their rights or requires further advice and guidance should contact the respective Campus Privacy Manager and/or the University Office of Privacy.

Anyone who receives a formal request from a data subject (verbal, written or via email) wishing to exercise any of the above rights must forward it immediately to the respective Campus Privacy Manager and/or to the Office of Privacy at the address below. The Office of Privacy must approve all proposed disclosures under a data subject access request (DSAR) before providing copies of personal data to the recipient.

8.0 Privacy by Design

The University is committed to ensuring privacy is built into its processes and outcomes. New projects involving personal data are required to carry out a data privacy impact assessment (DPIA) to identify privacy risks and plan appropriate mitigation. This process must be conducted whenever the University wishes to introduce the processing of existing personal data for new purposes, when introducing new business processes, selecting new IT applications, and/or engaging a new third-party vendor that includes the processing of personal data. University departmental managers must inform their Campus Privacy Manager or the Office of Privacy to initiate the assessment.

9.0 Information Security

The University has established an information security management system (ISMS) to recognize international standards to support compliance with the significant obligations to meet the "integrity and confidentiality" principle set out in the Regulation, including the obligation to notify the data protection supervisory authorities and, where necessary, data subjects in the event of a data breach. Details of the University's policies for information security are available at the dedicated information security SharePoint site.

10.0 Training and Awareness

The University is committed to ensuring its employees are provided with the requisite training and awareness around data protection and information security. All employees, faculty and adjunct faculty must undertake the mandatory data protection training annually.

11.0 Academic Research

Academic research, which involves the processing of personal data, is subject to approval by the University's Institutional Review Board (IRB) and includes specific instructions for assessing and maintaining privacy and security as a component of the IRB's approval process.

12.0 Responsibilities of All Data Users

12.1 *Lawful Processing*

All personal data is required to be processed in line with the lawful basis established by the University. Where special category data is processed, a second lawful basis is required.

12.2 *Retention of Personal Data*

Personal data must only be kept in a form which permits the identification of data subjects for no longer than is necessary and for the purposes for which the personal data is processed.

Personal data may be stored for longer periods when the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

The storage and retention measures are subject to implementation of appropriate technical and organizational measures to safeguard the personal data and data subject rights.

Further information about how the University stores and retains personal data, and for how long, can be found in the University's Data Retention Policy.

12.3 *New or Additional Processing*

Employees of the University (whether permanent or temporary) must not do any of the following without the proper authorization of their head of department and approval from the Office of Privacy:

a) Use other people's personal data that has been entrusted to the University for their own personal/private use, including the disclosure of personal data relating to colleagues, however well meaning.

b) Develop, purchase or subscribe to a new computer system/platform for processing personal data.

c) Use an existing computer system to process personal data for a new purpose.

d) Create a new electronic or paper filing system, including spreadsheets containing personal data, for a new purpose.

e) Engage a new vendor which will have access to, or process personal data (including its storage) on behalf of the University. The procurement or acquisition of all new software and systems, including cloud-based software as a service applications and free services involving the processing of personal data, is subject to strict evaluation and approval processes as part of procurement and the Global Privacy and Information Security Requirements which is part of Webster University´s Procurement Policy.

12.4 *Data Security Breaches*

All employees and constituents of the University are responsible for ensuring that:

a) Any personal data which they handle or process is held securely.

b) They are familiar with the University's latest information security policies relevant to their work and where to find them.

c) Personal data is not disclosed orally or in writing, or otherwise by any means, to any unauthorized third party, and that every reasonable effort is made to avoid personal data being disclosed accidentally.

d) All third-party requests for access to, or disclosure of, personal data, including those from the police and other law enforcement agencies, are directed to the Campus Privacy Manager or the University´s Office of Privacy.

e) Any unauthorized or accidental disclosure or misuse of personal data (whether real or suspected) is considered a data breach and is reportable to the Office of Privacy immediately on becoming aware.

f) Any recorded opinions about an individual are disclosable to them under a data subject access request and therefore need to be based on fact or professional opinion.

A breach of data protection law due to deliberate unauthorized access, data misuse, loss or destruction may result in disciplinary action, up to and including dismissal.

13.0 Responsibilities of Applicants and Students as Data Subjects

Applicants must ensure that any personal data supplied to the University is accurate and current, including changes of address and other contact details.

Students using University computing facilities are required to comply with the University's Acceptable Use Policy.

Students involved in organizing student unions, clubs and societies are also obliged to comply with the GDPR and similar legislation in force in the country of the University they are attending.

14.0 Responsibilities of Employees as Data Subjects

All employees must ensure that the personal data they supply to the University is accurate and up to date,

and that the University is informed of any errors in, or changes to, information which they have provided, e.g. changes of address or marital status. Changes can be made through the employee's assigned HR representative.

15.0 Closed Circuit Television

The University uses closed-circuit television (CCTV) and other video/electronic monitoring equipment as part of its measures to protect its campuses and its constituents. These monitoring systems are used in accordance with the Regulation and best practice standards and may be operated by third-party vendors on behalf of the University.

16.0 Sharing of Student personal data with Parents Guardians and Other Third-Parties

The University will not disclose personal data about its students to any third-party unless it has a clear and lawful basis for doing so (e.g. have a signed FERPA waver on file). This includes disclosure to parents, guardians and sponsors, including confirming that an individual is a student; to do so could infringe a student's rights to privacy and may, in extreme circumstances, place an individual in danger. Disclosure must only happen with the fully-informed written consent from the student for their information to be released to named individuals. In any case of doubt, please contact the respective Campus Privacy Manager of the University's Office of Privacy for guidance.

17.0 Data Protection Contact

Any questions relating to this Policy or requests for guidance should be directed to Webster University´s Office of Privacy at:

Webster University Office of Privacy
470 East Lockwood Ave., St. Louis, MO 63119
+1 314 246 7123
+43 1 269 92 93 4334
GDPR@webster.edu