

Office of Student Financial Aid

PRIVACY POLICY

Disclosure of Income and Tax information from the FAFSA with the applicant (and, if applicable, his or her spouse or parents) unless the FAFSA applicant (and, if applicable, his or her spouse or parents) can only be done after authenticate their identity.

Information about a student's financial aid is confidential and can only be given to the student directly or via mail. Only general information will be given over the phone or by e-mail. In addition, if the student is over the age of eighteen and is not claimed on the parent's taxes, no information can be released to the parent or guardian without a Financial Aid FERPA release.

Information Release In-Person

In order to disclose information from the FAFSA (income and tax information) to the student or parent in person, we must follow security protocols:

A FAFSA applicant (or custodial parent) appearing in person and presenting an unexpired, valid government issued photo identification (e.g. a driver's license, non-driver's identification card, other State issued identification, or U.S. passport) is a secure way of doing so for purposes of disclosing FAFSA information. A student can also present their RWU ID as a form of identification. For non-custodial parents or others (not on the FAFSA), we will require a FERPA Release form as well.

Information Release via Telephone

In order to disclose information from the FAFSA (income and tax information) to the student or parent over the phone, we must follow security protocols.

For student/ parent requests for information on the FAFSA, we must inform the student and/or parent that due to security reasons and for authentication, they /ormust idmgdenenthe sllow s FA0 -1.2Tc 0.002

In order to disclose financial aid information, the student and the custodial parent (if dependent) must sign a FERPA release form. The form states who is to receive the information. The student can rescind the consent in writing at any time. Copies of all consent documents are kept on file with the Registrar's Office. Financial Aid FERPA releases are kept by the Financial Aid office.

Data Security/Privacy Incidents

In order to protect personal information of residents of the Commonwealth of Massachusetts (201 CMR § 17.00) and residents of the State of Rhode Island (R.I.G.L. § 11-49.3-1), and in compliance with any other applicable law or regulation (the "Regulations"), Roger Williams University ("RWU") has developed the following Written Information Security Program (the "Program") to address the requirements of the Regulations.

The Program's goal is to set forth effective administrative, technical and physical safeguards for personal information; to provide an outline to assure the ongoing compliance with the Regulations; to protect personal information from unauthorized access, use, modification, destruction or disclosure; and to position RWU to comply with future privacy and safety regulations as such may develop.

To safeguard personal information, the Chief Security Officer will conduct a risk assessment. The initial risk assessment will seek to reveal the following potential and actual risks to the security and privacy of personal information:

- Unauthorized access of personal information by an employee not entitled to the information.
- Compromised system security as a result of unauthorized access by a third party.
- Interception of personal information during transmission.
- Unauthorized access to paper files containing personal information.
-

l-1]TJ94(1)u1.91 T/acd (d 11 >, i6e)4fh3(n)-2(hor)3• .

Disposal

RWU has implemented a record retention policy and schedule. When disposing of files containing personal information, RWU will follow its policy and schedule, which will include:

- Shredding all hard copies of files containing personal information when such information is no longer required or needed to be maintained by RWU.
- Destroying all electronic files containing personal information when such information is no longer required or needed to be maintained by RWU, including the destruction of residual electronic data on computers and other electronic devices.