

## Data Management

ISU data management policies pertain to all teaching and other professional activities of faculty and staff on behalf of ISU. Policies also apply to the use of personal devices used on campus for ISU business. Policies are available in the ISUPPs: 2410, 2420, 2430, 2440, 2450, 2480, 2490, 2500, 2510, 2520. The department's Administrative Assistant is our local guide to the implementation of these policies.

Generally, the following is the case: Local (not networked) data storage on ISU-tagged computer equipment is sufficient for storing grades. If grades are uploaded to Box, they should be regularly purged or stored in a FERPA-protected area within Box. For the department, the Administrative Assistant maintains a FERPA-protected area for any sensitive documents that we must retain.

Social Security Numbers are critical data and should not be stored except in FERPA-protected areas of Box. Materials containing SSNs should be deleted (if electronic) or shredded. Bengal numbers and Banner numbers are not critical data.

Faculty should also be sensitive to keeping materials in their offices and computer equipment secure through locking cabinets and doors when not in the office and through maintaining strong passwords for electronic equipment and for Box, changing passwords every 180 days. When using a publicly available computer, such as a classroom computer, faculty should always log out after use and deleting any downloaded and/or recycled files.