Qualtrics Data Management and Compliance

When using the university's Qualtrics system, users are responsible to comply with all JMU policies, standards and guidelines.

Collection of Personally Identifiable Data: Provided appropriate survey protocols are in place, Qualtrics can be used to collect personally identifiable data classified by JMU as **public** or **protected** (see JMU Policy 1205). Unless specifically approved by the University Data Managers Council, Qualtrics **may not** be used to collect personally identifiable data defined as **highly-confidential**—that which contains one or more of the following in association with an individual's name, email address, university or health identification number or other unique descriptor(s):

- Credit Card/Procurement Card Information
- Banking Information (account/routing detail)
- Social Security Number
- Driver's license number
- Visa number
- Passport number
- TIN/Vendor ID numbers that are SSN
- Biometric Identifiers (fingerprint, iris scan print, palm print, ear lobe map, etc.)
- Personal Health Information (includes but is not exclusive to HIPAA-protected data)

Human Subjects Research: The Institutional Review Board (IRB) must review and pre-approve any project where data is being collected for human subjects research.

For further assistance see:

- Institutional Review Board—Use of Human Subjects in Research
- Information Technology Policies, Standards and Guidelines

Data Security Consultation: Based on the types of data being collected along with the scope and more detailed requirements of your project, additional data security, compliance or technology system advice may be desirable. Consultation services are available to help guide individuals to the data handling and storage options most suitable to meet specific regulations and compliance requirements that may apply. To request such a consultation, submit a Technology Service Request (TSR) and you will be matched with an appropriate advisor.