Managing information is a shared responsibility. Information includes both electronic and physical records such as paper documents and files. The George Washington University’s Personal Information and Privacy Policy, Information Security Policy, and Records Management Policy guide faculty and staff in understanding the responsibilities and consequences of managing university information regardless of format.

What types of information need to be protected?

Regulated and Restricted data are considered non-public, meaning they are not intended to be shared with the general public and need to be protected from unauthorized access due to proprietary or privacy considerations. Its use or disclosure is governed under university policies, contract, or regulation. The chart below will help you determine the category of data you may work with in your role at GW.

- **Regulated Information** is protected by local, national, or international statute or regulation mandating certain restrictions. Examples include:
  - Personal health information
    - Past, present, or future physical or mental health condition
    - Provision of health care
  - Student academic and financial records
    - Grades/enrollment details
    - Financial aid student bills
    - Disciplinary action
  - Research data that is protected by statute or regulation
  - Personal data (any information relating to an identified or identifiable person)
    - Social Security numbers

- **Restricted Information** must be limited to appropriate university faculty, staff, students, or other authorized users with a valid business need. Examples include:
  - Course information/class schedules
  - Salary/benefits
    - Performance appraisals
    - Access codes
    - Wire transfers
    - Payment history
    - Legal records/contracts/legal filings
  - Financial records and accounts
    - General ledger data
    - Facilities/physical plant records
    - Library records
    - Accreditation records
    - GWid

- **Public Information** has no restrictions on access, use, or disclosure under university policy or contract, or under local, national, or international statute or regulation. Examples include:
  - Announcements/press releases
  - Public event information
  - Public directories and maps

How do I know if my GW computer, equipment or network is secure?

- GW’s Division of IT is primarily responsible for securing university-owned systems, equipment, and networks. You can help by protecting and securing your equipment and data and by utilizing strong passwords.

What am I responsible for?

- Understanding the requirements involved with having custody of certain types of data.
- Protecting, using, storing, and disposing of data properly.
- Using strong passwords on all devices

What are schools and divisions responsible for?

- Enforcing behaviors, processes, and practices to help protect university data.

Records management is essential to information management and required by the Records Management Policy. Schools and divisions are responsible for:

- Developing procedures and practices to manage records in their custody regardless of format.
- Securing non-public records in accordance with the Information Security Policy.
- Maintaining any records relevant to any pending or anticipated litigation, claim, audit, agency charge, investigation, or enforcement action.
- Transferring records of permanent value to University Archives.
- Disposing of records following the procedures for the Records Management Policy.

More information about types of data and how to protect it can be found on both the Compliance (compliance.gwu.edu) and Information Security (it.gwu.edu/information-security-and-compliance-services) websites.