SALISBURY UNIVERSITY

VI-14.00 POLICY ON PROTECTION OF SOCIOLOGICAL INFORMATION FROM INSPECTION AND DISCLOSURE

I. POLICY STATEMENT

This policy on the Protection of Sociological Information is intended to define the conditions under which Sociological Information shall be excluded from inspection and disclosure as part of a public record under Maryland's Public Information Act. The establishment of such a policy is referenced in USM BOR Policy VI-5.00 Policy on Inspection of Public Records.

II. PURPOSE

This policy is intended to define Sociological Information that shall be excluded from inspection and disclosure as part of a public record under the Maryland Public Information Act, Annotated Code of Maryland, General Provisions Article, §4-101 et seq. (the "Act").

The Act grants the public a broad right of access to government records. However, §4-330 of the Act provides, "If the official custodian has adopted rules or regulations that define sociological information…a custodian shall deny inspection of the part of a public record which contains sociological information…."

In accordance with the Act, Salisbury University (the "University") adopts this policy and defines University data that constitutes Sociological Information. Consequently, the University shall deny inspection, under the Act, of any and all records containing sociological information.

The exclusion of Sociological Information from public disclosure will serve to preserve the privacy of personal information and combat identity theft victimization of the University community.

III. APPLICABILITY

This Policy impacts all University community members including, but not limited to, students, employees, vendors, donors, or other individuals participating in a University program or event or using University facilities.

IV. DEFINITIONS

A. Sociological Information: is any information that may compromise, or be combined with other data to compromise, a University community member's personal information or put a University community member at risk of identity theft victimization.

B. University Community Member: includes, but is not limited to, students, employees, vendors, donors, and any individuals participating in a University program or event or using University facilities.

V. REQUIREMENTS

A. Pursuant to the Act, the University shall deny access to the following public record(s), or portion(s) thereof, containing Sociological Information of University Community Members, except as otherwise required by law. Sociological Information of a University Community Member includes the following information maintained by the University:

1. Scholarship, stipend and financial aid records of individuals or their families (to the extent this information is in the custody or control of the University);
2. Records about an individual's personal history, family, race, creed, color, religion, sex, gender, ethnicity, pregnancy, ancestry, age, gender identity or expression, physiology, national origin, veteran status, marital status, sexual orientation, physical or mental disability, or genetic information;
3. Family history, identity of relatives, emergency contacts or representatives;
4. Medical or Psychiatric history;
5. Social security numbers;
6. Date and place of birth;
7. Credit card and other banking information;
8. Personal addresses, personal phone numbers, personal electronic mail address and personal social media account information;
9. Information regarding marital status, domestic partnership dependents, or relatives;
10. Information regarding employment status, including disciplinary records ;
11. Records related to an application for employment;
12. Applications for admission, scholarship, stipend, or awards, including those of applicants who were either not selected/admitted or chose not to matriculate (to the extent this information is in the custody or control of the University);
13. Military service;
14. Driver's license number;
15. Class or employment attendance information;
16. State residency classification;

17. Immigration status, passport and visa numbers;
18. Religious preference, membership and attendance;
19. Personal relationships, belief and values;
20. Any information obtained through employment coaching or surveys;
21. Financial information, including income (excluding state salary), assets, and liabilities;
22. Donation and donor information, such as gift agreements, communications, and contact information for individuals or entities who have made charitable donations of goods, services, money or anything else to the University or the Salisbury University Foundation;
23. Student education records of a deceased student (to the extent that this information is in the custody or control of the University);
24. Program participation and community experience and activities (to the extent this information is in the custody or control of the University);
25. Records not related to the transaction of University or State business;
26. Records which contains political opinions, philosophical beliefs, and club/union memberships;
27. Unique biometric data or biometric information including an individual's physiological biological, or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity;
28. Internet or other electronic network activity information, including browsing history, search history, wireless network location data and information regarding an individual's interaction with an internet website or application; and;
29. Institutional identification number assigned to each applicant, student or employee (e.g. Workday ID, Employee ID, UID number) and photograph.

B. Information determined by the University to be "directory information" as that term is defined under the Family Educational Rights and Privacy Act of 1974 (FERPA) shall be provided in compliance with FERPA regulations.

VI. RESPONSIBLE OFFICE

The Office of General Counsel and the Office of the Registrar are responsible for the implementation and review of this policy.

Approved: July 25, 2019
Effective Date: August 1, 2019
Revised: March 1, 2023