**NORTHEAST COMMUNITY COLLEGE**

**ADMINISTRATIVE PROCEDURE NUMBER: AP-3511.3**

**FOR POLICY NUMBER: BP – 3511**

# PRIVACY AND RELEASE OF INFORMATION

## 1. PROCEDURE SUMMARY STATEMENT

To establish protocol pertaining to privacy and release of information.

## 2. DEFINITIONS

2.1 Personal Identifiable Information (PII) – any information relating to an individual or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly – in particular, by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.

2.2 Family Educational Rights and Privacy Act (FERPA) – a Federal law that protects the privacy of student education records.

2.3 Education Record – a record that contains information directly related to a student and which are maintained by an educational agency or institution or by a party acting for the agency or institution. See 34 CFR Section 99.3 for a complete definition of "education records" and a list of records that are not included in the definition.

2.4 Free Application for Federal Student Aid (FAFSA) – a form completed by current and prospective college students (undergraduate and graduate) in the United States to determine their eligibility for student financial aid.

2.5 Protected Data – encompasses information deemed confidential or restricted under federal or state law or rules, the College's contractual obligations, or privacy considerations such as the combination of names with respective Social Security Numbers.

2.6 Private Data – information for which the unauthorized disclosure may have moderate adverse effects on the College's reputation, resources, services, or individuals. This includes data classified as Internal.

2.7 Public Data – information for which disclosure to the public poses negligible or no risk to the College's reputation, resources, services, or individuals. This is the default classification, and should be assumed when there is no information indicating that information should be classified as protected or private. In addition, certain legislation may specify select information as public.

2.8 Data Steward – an employee who oversees the capture, maintenance and dissemination of data for a particular operation.

2.9 Information Custodian – an employee responsible for specifying the security properties associated with the information assets their organization possesses. This includes categories of information that users are allowed to read and update.

## 3. PROCEDURE

3.1 Authorized Users of Protected or Private Information

3.1.1 Access to Northeast Community College (Northeast) information classified as protected or private requires appropriate authorization:

3.1.1.1 It is the responsibility of the designated data steward to authorize access to protected or private information to users or entities as required for them to perform their assigned job duties, to complete a business process, or by contractual obligation. Legal or regulatory requirements may impact who is authorized to view Northeast protected or private information access.

3.1.1.2 For an individual not employed by the College, or third parties who are authorized to view protected or private information as part of a regulatory, academic, or business function, the sharing Northeast unit must have a signed Non-Disclosure Agreement on file for individuals or Northeast data sharing terms and conditions for third parties. Additionally, background checks may be required prior to granting access to Northeast protected or private information.

3.1.1.3 The individual whose protected or private information is produced or displayed is authorized to access that information unless restricted by legal or contractual obligations.

3.2 Confidentiality Statement and Privacy Training

3.2.1 Signed Employee Non-Disclosure Agreement and training are required for Northeast employees with authorization to access or process protected or private information. The position description for each Northeast position involving access to protected or private information must reflect the access requirements. Employee Non-Disclosure Agreement must be maintained on file in the Human Resources office and be available for audit. This information may be stored in a digital or paper format.

3.2.1.1 Employees designated as having access to select protected information (e.g., HIPAA) may be required to sign agreements acknowledging special confidentiality controls necessary to meet specific legal or contractual privacy requirements. These agreements are in addition to a signed Northeast Employee Non-Disclosure Agreement document.

3.2.1.2 Each department must train its employees on the requirements to safeguard protected or private information. This training should occur prior to unsupervised employee access of protected or private information or as required by legislation or contractual obligation.

3.3 Approved Transfer of Protected or Private Information

3.3.1 The following actions involving protected or private information must be authorized by the responsible Dean, Director, Department Head, or designee and related approval documentation maintained on file at Vice President of Technology Service's office:

3.3.1.1 Transferring between Northeast computing resources and third-party vendors or service providers.

3.3.1.2 Transferring to portable storage, portable computing devices such as laptop computers, tablets or smartphones.

3.3.1.3 Allowing information custodians to access information to perform an approved action to mitigate a system problem or as part of an incident response to a privacy breach investigation.

3.3.2 The Executive Vice President maintains guidelines for a response to a legal demand including a valid subpoena, warrant, legal order, to meet a legal or contractual order for the transfer of protected information. These guidelines will govern a response, reply, or appearance to a legal demand.

3.4 Third-party access to Protected or Private Information

3.4.1 The College may choose to contract with a third-party for the collection, storage, or processing of information, including protected or private information. The third-party may offer services in the form of hosting, outsourcing, or private/public cloud computing services.

3.4.2 All Northeast contracts with a third-party for the processing of protected or private information must be regulated by a detailed, written agreement, in which the rights and duties of the College and the third-party contractor in addition to any subcontractors engaged by the primary third-party contractor are specified. The College shall select a third-party contractor that will strive to adhere to the technical and organizational security/privacy measures required in this privacy procedure and provide reasonable assurance with respect to the protection of the information.

3.4.3 A third-party contractor shall also be contractually obligated to process protected or private information only within the scope of the contract and the directions of the College. Processing of protected or private information may not be undertaken for any other purpose.

3.5 Physical Security Access Restrictions

3.5.1 Offices and storage facilities that maintain protected or private information locally must ensure all protected or private information is secured using proper storage methods. This includes but is not limited to locked cabinets and drawers for hardcopy or electronic devices (such as laptops, phones, tablets, CDROMs, DVDs, USB flash drives) when not in use. Documents and media containing protected or private information shall be shredded, physically destroyed or wiped by electronic methods to render the information unreadable and unrecoverable as stipulated in National Institute of Standards and Technology-Special Publication 800-88 Revision 1 Guidelines for Media Sanitization.

3.5.2 Additional physical privacy controls may also be required by law or contractual obligation for specific information items.

3.6 Protected or Private Information Use in Social Media

3.6.1 It is important to recognize that the same laws, policies, rules of conduct and etiquette that apply to all other activities at or concerning the College also govern the use of social media. Because of the powerful ability of social media to broadcast information worldwide, faculty and staff should safeguard all protected or private information – only posting what you have permission to post by law, policy or explicitly.

3.6.2 Employees who use social media within their duties or coursework should consider student privacy carefully, including compliance with the Family Educational Rights and Privacy Act (FERPA). Most information that identifies a student and is maintained by the College, or by an educator or agent of the College, is protected under FERPA. This protection extends to postings of any information item considered to be part of a student's education record on social media course accounts. A signed FERPA release for a specific activity must be retained by the campus entity to publicly post information considered a protected education record.

3.7 Protected or Private Information Use in Photography and Videography

3.7.1 Certain photos and videos of students are "educational records" under FERPA, and cannot be shared publicly without the written consent of the student. Consent is particularly important where photos or video images identify students in their academic courses.

3.7.2 Class recordings may raise privacy concerns due to FERPA regulations. In cases where class-recording videos are made accessible only to the students and instructors in the class and academic administrators, students should be informed of the video recording in advance. Within a class or even outside of the classroom, if a student or students are identifiable in a photograph or video,

FERPA may apply and require that permission be obtained before the photo or video is shared publicly.

3.7.3 Student use of electronic devices, including wearable computing devices, capable of photography, audio, or video recording of events are prohibited during certain classroom functions, research activities, or supporting business processes involving information classified as protected or private. Examples of prohibited uses include academic functions such as examinations, unapproved use in healthcare functions covered by HIPAA, and research functions where contractual or legal rules restrict information sharing.

3.8 Use of Biometric Technologies

3.8.1 College units implementing biometric technologies must ensure they meet any relevant privacy and biometric laws and regulations as they may relate to the acquisition and retention of biometric information. In addition, the College unit must ensure that its use meets a defined business need with auditable procedures to secure the biometric information and privacy of the enrollees.

3.9 Online Collection of Protected and Private Information

3.9.1 Campus units that collect protected or private information on their public or Intranet web pages must ensure technical controls provide encryption of protected information communicated between a user's browser and a web-based application through the use of secure protocols (e.g., HTTPS, TLS/SSL, etc.). In addition, any storage of protected or private data on publicly accessible webservers must be encrypted. The College's websites collecting protected or private information require a link to the Northeast Privacy Policy.

3.9.2 Prospective students, current students, faculty, staff, and interested parties residing outside of the United States and providing protected or private information electronically to the College understand this information will be transferred to the U.S. where it will be processed and stored under U.S. privacy standards or by applicable framework agreements.

4. Standards for specific information types

4.1 Public Records

4.1.1 Northeast faculty, staff, and contracted business partners must ensure the safekeeping of public records that have archival, administrative, or legal value. The Northeast Records Management Policy BP-3070 contains specific responsibilities for the retention, storage, disposal, and archival of the College's records.

4.1.2 The College recognizes the importance of providing full access to public records at the request of citizens and the news media to ensure confidence in the

institution. Nebraska State law defines what a public record is and excludes confidential data.

4.1.3 Nebraska State Statutes (84-712 to 84-712.09) provide, in summary, for:

4.1.3.1 The examination of public records at no charge during regular business hours.

4.1.3.2 The payment of actual cost for the making of photocopies of original public records.

4.1.3.3 The payment of the actual cost, for electronic data, including reasonably calculated actual cost of computer run time, any necessary analysis and programming, and the production of the report in the form furnished.

4.1.3.4 A deposit from the requester prior to the fulfillment of the request in cases where the production of the public records is estimated to exceed $50.

4.1.3.5 Requests to be fulfilled not more than four business days after the actual receipt of the request or, in cases where fulfillment is not possible in that timeframe, a written explanation stating when the request can be fulfilled, an estimate of the cost, and an opportunity for the requester to modify the original request.

4.1.4 The College is not required to produce or generate any public record in a new or different form or format modified from that of the original public record; however, where practical and affordable such requests may be honored. Practical and affordable requests are those that do not interfere with the normal operation of the College nor place an undue financial burden on the College to be complied with. In most cases the requester shall pay for the cost of such public record request in full. In exceptional cases, where the President or his or her designee deems the request to be central to the public's right to know, the cost of a public records request may be discounted or waived.

4.1.5 While all Nebraska citizens have the right to access public information, the College will attempt to honor requests for information not in original form or format made by those providing information to a broad base of Nebraska citizens.

4.2 Student Education Records

4.2.1 Student education records are classified as Protected for Northeast records. The Family Educational Rights and Privacy Act (FERPA) is a federal law that protects the privacy of student education records. FERPA affords students attending a postsecondary institution certain rights with respect to their education records. More information regarding the Northeast guidelines for

application of FERPA are available through the office of the Vice President of Student Services.

4.2.2 Rights afforded by FERPA

4.2.2.1 The right to inspect and review the student's education records within forty-five (45) days from the day the College receives a request for access. The student must submit to the Registrar a written request identifying the record(s) they would like access to. The Registrar will make arrangements with the Vice President of Student Services and appropriate Student Services Dean(s) or other appropriate officials, and notify the student of the time and place the records may be accessed. The College will provide the student with copies of educational records or otherwise make the records available to the student if the student lives outside of reasonable commuting distance of the College.

4.2.2.2 The right to request an amendment of the student's education record that the student believes is inaccurate. The student must notify in writing the Northeast official responsible for the record, clearly identify the part of the record they want changed, and specify why the record is inaccurate. If the College decides not to amend the record as requested by the student, the student will be notified of the decision and advise the student of their right to a hearing regarding the request for amendment. Additional information regarding the hearing procedures will be provided to the student when notified of the right to a hearing.

4.2.2.3 The right to provide written consent before the College discloses personally identifiable information (excluding directory information, see below) from the student's education records, except to the extent that FERPA authorizes disclosure without consent.

4.2.3 The College is authorized under FERPA to release directory information which includes the student's name, address (mailing and email), telephone number, program of study, participation in officially recognized sports and activities, weight and height of athletic team members, terms of enrollment, certificates, diplomas, or degrees conferred, College honors and awards received, enrollment status (full-time or part-time), photographs, and the most recent previous institution attended by the student. This information may be released by the College at any time. If a student does not desire directory information to be released, a request in writing must be filed with the Admissions and Registration Office. Release of any information, other than directory information, requires written permission from the student. This permission must be signed and dated by the student, list what records are to be released, the purpose of the disclosure, and to whom the disclosure should be made. If a student so requests, a copy of the disclosure must be given to the student.

4.2.4 The College will annually notify students in attendance of their FERPA rights. The annual notice will be available on the College website, the Student Handbook and Planner, and the College Catalog.

4.2.5 The right to file a complaint with the U.S. Department of Education concerning alleged failures by the College to comply with the requirements of FERPA. The name and address of the Office that administers FERPA is:

Family Policy Compliance Office
U.S. Department of Education
Maryland Avenue, SW
Washington, DC 20202-4605

4.3 Student Financial Aid Records

4.3.2 The Northeast Financial Aid Office is entrusted with highly sensitive information about each student and their family in the course of assisting with the application for and processing of requests for aid. Employees are obligated to safeguard this information in compliance with applicable laws that govern access to, disclosure of and use of student financial aid information. These applicable laws include The Higher Education Act of 1965, as amended (HEA) and The Privacy Act of 1974, as amended (Privacy Act).

4.3.3 The HEA specifically restricts the use of FAFSA data and states that data collected on the FAFSA form shall be used only for the application, award, and administration of aid awarded under federal student aid programs, state aid or aid awarded by the institution. Because of HEA, the financial aid office will not disclose information collected from a student's FAFSA or financial aid award or eligibility to any third party person (including parents or spouses) or entity requesting this data on the student's behalf without explicit written consent.

4.3.4 The Privacy Act governs the collection, maintenance and use of records maintained by federal agencies and generally prohibits agencies from disclosing data contained in those records. The Privacy Act can impose restrictions on institutions as well if a federal agency lawfully provides records or access to records to an institution.

4.4 Social Security Numbers

4.4.2 Social Security Numbers are classified as Protected for Northeast records. The College collects and stores Social Security Numbers (SSNs) as permitted by law. College units and their employees are only permitted to collect or store SSNs when necessary to meet a state or federal requirement or the unit has obtained written approval from the President, Vice President, General Counsel, Information Security Officer, or designated approver to meet an official business process.

4.4.3 The College requires all entities maintain privacy controls over SSNs to meet legal, contractual, or good privacy practice requirements.

4.5 Health Insurance Portability and Accountability Act (HIPAA Privacy Rule)

4.5.2 The HIPAA Privacy Rule (45 CFR Part 160 and 164) provides protections for individually identifiable health information held by covered entities and their business associates and gives patients an array of rights with respect to that information. This information is classified as Protected for Northeast records.

4.5.3 Each Northeast entity designated as a HIPAA "Covered Entity" or "Business Associate" as defined by the US Department of Health and Human Services (http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html) will appoint a HIPAA Privacy Officer. The Privacy Officer is the entity's administrative resource for implementation and compliance with the current requirements of the HIPAA Privacy Rule.

4.6 Gramm-Leach-Bliley Financial Modernization Act of 1999 (GLBA)

4.6.2 The College generates, receives and stores many financial documents and records classified as protected. This includes, but is not limited to, information about the awarding and issuance of loans to students, and the collection of payments from students, parents, patients and customers via check, money order, wire transfer, Automated Clearing House (ACH) and credit/debit card. GLBA (Public Law 106-102) applies to any record handled or maintained by, or on behalf of, the College or its affiliates that contains protected financial information about a student or other third-party who has a relationship with the College.

4.6.3 GLBA safeguarding provisions pertain to any record containing protected financial information whether in paper, electronic or other form, which is handled or maintained by or on behalf of the College or its affiliates. For these purposes, the term protected financial information shall mean any information (i) a student or other third-party providers in order to obtain a financial service from the College, (ii) about a student or other third-party resulting from any transaction involving a financial service, or (iii) otherwise obtained about a student or other third-party in connection with providing a financial service to that person. In particular, safeguarding provisions of this procedure and the College's security policy (i) ensure the security and confidentiality of covered records, (ii) protect against any anticipated threats or hazards to the security of such records, and (iii) protect against the unauthorized access or use of such records or information in ways that could result in substantial harm or inconvenience to customers.

4.6.4 All Northeast contracts with third-party providers who are responsible for processing, transferring, or storing GLBA-protected information will be required, under the terms of the contract, to stipulate implemented safeguards that adhere to, and are in compliance with, the provisions of the Gramm-Leach-Bliley Act.

4.7 General Data Protection Regulation (GDPR)

4.7.2 The College processes personal data both as a Processor and as a Controller as defined in the GDPR. This personal data is classified as Protected for such records. Privacy notices, consent and rights regarding the lawful base(s) for processing data must be given at the time of collection.

4.7.3 Questions regarding the College's collection and storage of data can be submitted to:

Northeast Community College
Information Security Office
801 E. Benjamin Ave.
Norfolk, NE 68701

4.8 Payment Card Industry Data Security Standard Transactions

4.8.1 The College will only collect and use information obtained from branded credit/debit card transactions (VISA, MasterCard, and Discover) only for business purposes upon approval by the Executive Director of Finance. The credit card information is classified as Protected for Northeast records, and will be safeguarded in a confidential manner as defined in Northeast Credit Card Handling Protocol and as specified in the merchant agreements as contractual obligations. Such obligations include compliance with the Payment Card Industry – Data Security Standard (PCI DSS).

4.9 Electronic Communications / E-Mail

4.9.2 E-mail and electronic communications are classified as Private for Northeast records. Confidentiality and privacy cannot be guaranteed through electronic communications because of the nature of the medium and the accountability as a public institution. The College supports a climate of trust and respect and does not ordinarily read, monitor, or screen instant messaging, voice mail, or electronic mail services provided by the College.

4.9.3 The President's designee may authorize access to faculty, staff, or student instant messaging archives, voice mail, or email in a number of circumstances including, but not limited to health and safety, conduct and disciplinary actions, violations of legal or contractual obligations, or critical processing of business operations.

4.9.4 E-mails containing information classified as protected should use encryption or password protect the document as an attachment.

5. Privacy violations and reporting

5.1 Privacy violations occur when a Northeast student, staff, contractor or faculty member violates this procedure, specific legal privacy requirements, or contractual obligations. For the purpose of this procedure there are three primary classifications of privacy violations at the College:

5.1.1 Incidental disclosure which occurs when an unauthorized party overhears or sees protected or private information during a permitted use or disclosure in a work space.

5.1.2 Accidental disclosure occurs when privacy control weaknesses allow unauthorized access to protected or private information. Privacy control weaknesses include human error or a fault in privacy control procedures that leads to a loss of ability to limit access to protected or private information to only authorized users.

5.1.3 Intentional disclosure occurs when privacy controls are overridden to allow unauthorized access or disclosure of protected or private information. This can be done with or without malicious intent.

5.2 It is the responsibility of each Northeast student, staff, contractor, or faculty member to immediately report suspected or confirmed violations to their supervisor or contract administrator including accidental disclosures. If the supervisor or contract administrator is unavailable or if there is a potential conflict of interest, the report should be directed to the Dean, Director, Department Head, Director of Technology Risk & Service Management, or through the Northeast Service Center. The Dean, Director, or Department Head must inform the Director of Technology Risk & Service Management of any suspected or confirmed privacy violations within 24 hours. Refer to the Director of Technology Risk & Service Management for incident management.

## 6. APPLICABILITY

N/A

**ISSUE DATE:** 04/24/2019
**EFFECTIVE DATE:** 04/24/2019
**REVISION DATE(S):** none
**PRIOR POLICY/PROCEDURE NUMBER:** none
**SCHEDULE FOR REVIEW:** 2024
**DIVISIONS/DEPARTMENT RESPONSIBLE FOR REVIEW & UPDATE:** Technology Services
**SPONSORING DIVISION/DEPARTMENT:** Technology Services
**RELATED PROCEDURES/ REFERENCE:** AP-3511.0; AP-3511.1; AP-3511.2; AP-3511.4
**PROCEDURE KEY WORDS:** student privacy; release of information; FERPA; GLBA; PCI DSS