

Section:	VIII.2.9	
Title:	Electronic Records Privacy and Access - Interim	
Effective Date:	September 4, 2019	
Approved By:	President	
Responsible Unit:	Office of the General Counsel (609) 771-2734; privacy@tcnj.edu	
Related Documents:	<ul style="list-style-type: none">• Computer Access Agreement• Family Education Rights and Privacy Act (FERPA) Policy• Information Classification Policy• Information Security Policy• Email Investigation Guidelines	
History:		
Version	Date	Notes
2.0	9/4/19	Revision of Interim Policy (prior to governance review)
1.0	5/21/19	New policy; initial release

I. INTRODUCTION

Students, faculty, and staff of The College of New Jersey (the “College” or “TCNJ”) regularly rely on technology including Electronic Records to efficiently perform many aspects of their work, including teaching, research, study, and other activities. Much of this work may be conducted using College Systems. TCNJ is committed to the privacy of its students, faculty, and staff, however, TCNJ reserves the right to access Electronic Records as described herein. This policy provides information on the privacy of and access to Electronic Records.

II. DEFINITIONS

College Systems – Electronic or digital accounts, systems, networks, services and devices owned, administered, and/or maintained by the College, including, without limitation, computers, smart phones, shared drives, e-mail accounts, and other TCNJ licensed software and system accounts.

Compelling Circumstances – Circumstances in which failure to act may result in bodily harm, property loss or damage, loss of evidence or violation of law or of College policy, or liability to the College or to a student, faculty, or staff member.

Electronic Records – Messages, transmissions and data, metadata, including, telephone records, e-mail, voice mail, data files and other electronic and digital

communications and other records, that are created, sent, forwarded, replied to, transmitted, distributed, broadcast, stored, held, copied, downloaded, displayed, viewed, read, or printed by or with College Systems. This definition includes and applies equally to the contents of such records, attachments to such records, and transactional information associated with such records.

Emergency Circumstances – Circumstances in which time is of the essence and it is more likely than not that delaying action would result in Compelling Circumstances.

User(s) – College faculty, or others holding academic appointments at the College, students, and staff, who create, send, forward, reply to, transmit, distribute, broadcast, store, hold, copy, download, display, view, read, or print Electronic Records.

III. POLICY

A. Electronic Records Privacy

The College takes reasonable steps to protect Electronic Records from unauthorized access. College employees are required to follow all applicable policies and procedures governing the privacy, confidentiality, and security of data, including Electronic Records. However, users should be aware that certain Electronic Records and College Systems (e.g., e-mail) by their nature may not be fully secure and may be vulnerable to impermissible and/or illegal access.

B. Permitted Access

Permitted Access to a User's Electronic Records is treated with the utmost seriousness, consonant with the College's interest in maintaining an environment in which free academic inquiry thrives.

The scope of the information accessed must be limited to the purpose of the Permitted Access and limited to those individuals who need to review it for that purpose. Permitted Access shall be content and viewpoint neutral of the User's speech or expression, provided such speech or expression does not violate applicable laws or policies. Further, the Permitted Access will be focused on the purpose of the review.

The College may access and monitor a User's Electronic Records in connection with the following (collectively, "Permitted Access"):

- i. Without User Consent if any of the following situations occurs or applies:
 - a. an investigation for alleged misuse and/or abuse of College Systems;
 - b. an alleged violation of law or College policy;

- c. the maintenance of the performance, operation, or security of College Systems, or troubleshooting of network or account problems by authorized personnel within the Office of Information Technology (IT);
 - d. Open Public Records Act (OPRA) or Freedom of Information Act requests submitted to the College's Records Custodian;
 - e. requests submitted in compliance with Family Education Rights and Privacy Act;
 - f. investigation or collection of data for an internal College process such as grade appeal, employee discipline matters, library financial obligations in accordance with *N.J.S.A. 18A:73-43:2* and student conduct matters;
 - g. subpoenas, court orders, warrants, or other legally mandated processes; or
 - h. other Compelling Circumstances.
- ii. With User Consent if:
 - a. the User has provided consent to access to the User's Electronic Records.

Requesting Access to Electronic Records

1. Access With Consent

Upon receiving consent from the User and prior to accessing any Electronic Record, the requestor must submit the completed **Consent to Access Electronic Records** form (Attachment A)¹ to the Privacy Office. Any User who receives a request for consent that they believe is unreasonable or feels that their consent was granted under duress, should immediately notify the Privacy Officer. The Privacy Officer may: (i) approve the requested access, (ii) approve access, but place additional limitations on the requested access (for example if the requested access was overly broad); or (iii) in cases of suspected abuse, duress or insufficiently justified need, deny access.

2. Access Without Consent

When Electronic Records are to be accessed without the User's consent, such action must be requested and ultimately authorized for access by the appropriate authority as outlined in Section D. below. Requestors must complete the **Request**

¹ The Privacy Officer is authorized to modify the form of the Consent to Access Electronic Records consistent with this policy

for Access without Consent form (Attachment B) .², obtain approval of such request from his or her unit's Vice President or Senior Administrator, and if approved, submit the completed form to the Privacy Office for review and consideration.

The Privacy Officer is responsible for coordinating the review of any requests under this policy for access to Electronic Records without the consent of the User.

C. Authorization of Access

Upon receipt of the completed Access without Consent Request form, the Privacy Officer shall review the request and recommend whether to permit, permit with modification, or deny access to the Electronic Records. If legal review is necessary as determined by the Privacy Officer, the Privacy Officer shall forward the request to the Office of the General Counsel for review and recommendation.

Upon reviewing the recommendations of the Privacy Officer and Office of the General Counsel (if applicable), final review and authorization shall be as follows:

1. **Faculty** - If the User is a faculty member or other holder of an academic appointment at the College³, the authorization of the Vice President for Academic Affairs/Provost must be obtained; provided, however, that if the Vice President for Academic Affairs/Provost is the requesting Vice President under Sec III C. 2., the authorization of the Vice President for Human Resources must be obtained.
2. **Staff (non-faculty)** - If the User is an employee other than a faculty member the authorization of the Vice President for Human Resources must be obtained; provided, however, that if the Vice President for Human Resources is the requesting Vice President under Sec III C. 2., the authorization of the Vice President for Academic Affairs/Provost must be obtained.
3. **Student** - If the User is a student, the authorization of the Vice President for Student Affairs must be obtained; provided, however, that if the Vice President for Student Affairs is the requesting Vice President under Sec III C. 2., the authorization of the Vice President for Human Resources must be obtained.

² The Privacy Officer is authorized to modify the form of the Request for Access without Consent consistent with this policy

³ If the individual is adjunct faculty or holds concurrent faculty rank, but the request relates to that individual's staff employment position, the Privacy Officer shall determine whether the request should be treated D.1. Faculty or D.2. Staff (non-faculty).

Once a final decision on authorization has been made, the completed request form shall be returned to the Privacy Officer whom shall notify the requestor of the decision on authorization of access. The Privacy Officer shall store and maintain the completed Request Form for record keeping. Any documentation supporting the review and final determination of access shall be maintained with the request form.

Any authorization of access shall apply only to the particular circumstance and User as requested. Any other instances of access must be separately authorized.

No authorization is required for IT to access Electronic Records to maintain the performance, operation, or security of its systems, or to troubleshoot network or account problems.⁴ Likewise, requests for access in connection with litigation, legal processes, or law enforcement investigations, or to preserve User Electronic Records need no authorization if requested by the Office of the General Counsel.⁵

D. Emergency Access

In Emergency Circumstances, the least access and least action necessary to resolve the emergency may be taken immediately without authorization, but appropriate authorization must be sought without delay as required in Section C. and Section D.

E. Oversight Committee

This policy, its implementation, and instances of access under this policy shall be subject to review by an oversight committee to be established by the College, which shall include faculty and senior administrators. The oversight committee shall make recommendations to the President as to the implementation of the policy and possible amendments. In carrying out its responsibilities, the oversight committee may review the records described in Section C. and Section D. of this policy, subject to redaction as necessary to protect individual Users.

F. Violations of this Policy

Failure to follow proper policies and procedures concerning Permitted Access to Electronic Records may result in disciplinary action.

Students, faculty, or staff who believe that this policy has been violated should report such violations to the Privacy Officer.

⁴ See the College's *Computer Access Agreement*.

⁵ See the College's *Receipt of Legal Documents and Contacts from Outside Legal Authorities* policy and the *Legal Hold* policy for further information.

Attachment A

Consent to Access Electronic Records

Name of User (Individual): _____

Name of Requester (Individual Seeking Access): _____

User Status: ☐ Student ☐ Faculty ☐ Staff ☐ Other

College System Name(s)/Description: _____

Electronic Records Sought: _____

From Date: _____ To Date: _____

Subject/Description of Electronic Records Sought: _____

DESCRIPTION OF PERMITTED ACCESS

Provide a description of the need to access the requested Electronic Records as permitted under Section B., Permitted Access, of the policy:

Timeframe of Access Authorization:

- ☐ for the duration as needed (no timeframe restrictions)
- ☐ expires on ____/____/20____ (expiration date)

Additional Comments/Limitations/Instructions (if any):

Consent Approval:

I hereby consent to provide access to the above electronic records by all parties deemed necessary and appropriate by The College of New Jersey Privacy Officer. I understand that the scope of the information accessed will be limited to the purpose of the Permitted Access and limited to the number of people who need to review it for that purpose as required under the College's Electronic Records Privacy and Access policy. I further understand that I may revoke my consent at any time via written notice to the Privacy Officer.

Printed Name	Signature	Date

Scan and submit **signed form** to privacy@tcnj.edu.

For assistance, contact Aminah Massenburg, Privacy Officer at massenba@tcnj.edu.

Attachment B

Request for Access without Consent

The College of New Jersey's *Electronic Records Privacy and Access* policy provides that the College does not access Electronic Records without the User's consent, except under limited circumstances and with appropriate authorization.

Note: Meeting the provisions detailed below does not guarantee approval for access.

SECTION 1) Section 1, A through D to be completed by requestor. Scan and submit signed form to privacy@tcnj.edu. For assistance, contact Aminah Massenburg, Privacy Officer at massenba@tcnj.edu.

A) REQUESTED RECORDS:

Name of User (Individual): _____

Name of Requester (Individual Seeking Access): _____

User Status: ☐ Student ☐ Faculty ☐ Staff ☐ Other

College System Name(s)/Description: _____

Electronic Records Sought: _____ From Date: _____ To Date: _____

Subject/Description of Electronic Records Sought: _____

B) DESCRIPTION OF PERMITTED ACCESS:

Provide a description of the need to access the requested Electronic Records as permitted under Section B., Permitted Access, of the policy:

C) REASON WHY CONSENT CANNOT OR NEED NOT BE OBTAINED:

- ☐ The User cannot be contacted because of absence or illness.
- ☐ The User has denied or failed to timely respond to a request to access the specified College records.

☐ User Consent is not required because the request meets the requirements of Section III. B (i) of the Policy. List particular applicable subsection with explanation:

☐ Post-authorization: the Electronic Records have already been accessed under **Emergency Circumstances** (Circumstances in which time is of the essence and there is a high probability that delaying action would almost certainly result in Compelling Circumstances.) Provide explanation: _____

D) REQUESTED BY: DEPARTMENT/UNIT: _____
CONTACT: _____

Approval by Requesting Unit Vice President or Senior Administrator:

Signature _____ Print Name _____ Date: ____ / ____ / ____

SECTION 2) REVIEW by Privacy Officer (required for all requests):

IS NON-CONSENSUAL ACCESS RECOMMENDED? ☐ YES ☐ NO

COMMENTS: _____

Signature _____ Print Name _____ Date: ____ / ____ / ____

SECTION 3) REVIEW by Office of the General Counsel (as applicable)

IS NON-CONSENSUAL ACCESS RECOMMENDED? ☐ YES ☐ NO

COMMENTS: _____

Signature _____ Print Name _____ Date: ____ / ____ / ____

SECTION 4) CAMPUS AUTHORIZATION

☐ For Student Record Holders: Vice President for Student Affairs

☐ For Faculty Record Holders: Vice President for Academic Affairs/Provost

☐ For Staff (non-faculty employees): Vice President for Human Resources

Do you authorize access to Electronic Records as requested above: ☐ YES ☐ NO

Provide a brief explanation of the authorization decision:

Printed Name	Signature	Date