EAST CENTRAL COLLEGE

Request for Colleague and Perceptive Content

Employee Access Information

Employee Name: ________________________________ Employee ID/SSN: ______________________________

Title Department: _______________________________ Immediate Supervisor: ___________________________

Is this person replacing an employee who had access? □ Yes □ No

If yes, who _______________________, and did this person leave this position for another at ECC □ Yes □ No

Access to Data

Check the blanks of the data categories below that pertain to the kind of access needed. The access to information must relate to the responsibilities of the person.

Please note that all employees will be given access to the new online access to Colleague (eCentral).

Category	**Inquiry**	**Update**
Student Information	□	□
Financial Aid	□	□
Financial Services	□	□
Human Resources/Payroll	□	□

Other (please specify) _____________________

Will this person also need access to Perceptive Content? □ Yes □ No

Acceptance of Responsibility

I understand my acceptance of access to the College-wide information system signifies I accept the responsibility for complying with the institutional policy for Release of Information. I have been given copies of and have read the Release of Information policy and the Explanation of Access to guidelines. By my signature below, I understand and agree to preserve the security and confidentiality of information I access.

I understand I am responsible for the personal security of my password.

_______________________________________ ___________________________

Signature of Employee Date

I am responsible for providing an orientation for the employee or making arrangements with proper personnel to provide orientation. I will inform the Information Technology Department of any change in status of this employee. I will initiate access deletion if this employee leaves the current position for which he/she has been given approval, and will initiate a new Access Request document for this employee's replacement, if appropriate.

_______________________________________ ___________________________

Signature of Supervisor Date

Cc: IT Department 06/19/2018

EXPLANATION OF ACCESS (Employee should keep this section for reference.)

The procedure to obtain access to data are in compliance with federal government ("Family Educational Rights and Privacy Act of 1974") (FERPA).

What is (online) view access? Online access is a tool by which certain information stored on computer files may be viewed on a computer terminal/pc. Information accessible to authorized individuals includes data and other information. Online access allows an authorized user the opportunity to view information on specific students and courses. In addition, some data may be updated by authorized individuals.

Who may request access? Security of restricted data is a matter of major concern. Approval for access will be evaluated based upon a "legitimate need to know" the information as outlined in the "Release of Student Information Policy".

It is the responsibility of the supervisor to train new staff in his/her department and share access information with staff who have access.

What is the access request procedure and approval process? Before approving access to restricted data, a Request for Access document must be completed for each individual who is to have access.

The supervisor sends a completed Request for Access form to Human Resources. Each request for access is individually evaluated by the Information Technology Department. It is expected that only those persons identified on the request form will have access to the system; therefore, access must be requested for each person in order to maintain systems security. Access is issued to a person, not a position or a workstation.

What are the responsibilities of persons with access? Each person approved for access is responsible for security of his/her password and protection of information. The authority to access is linked to a person's ID and password on the Colleague system. At no time should any individual share his/her password with another person or display the password in public view. Each person approved for access is responsible for signing off when finished with access.

Further, it is the understanding that student records information available through access will be employed only for the purpose for which it was requested and will not be released to any other individual or office for another purpose. A person having access to student records should be aware that there are possible civil sanctions for violating records privacy agreements.

All persons accessing confidential student data must guarantee to maintain data about individual students in a secure fashion, such that it cannot be viewed-by screen access, file access or in printed form-by unauthorized individuals. Although it is allowable to print a report or screen of confidential information for authorized recordkeeping or advising purposes, the user should not release the printed information to other individuals or offices. Any personally identifiable confidential data contained in print form or on computer files which are no longer need should be destroyed in such a way that identification of a student is not possible.

As part of the request process, each person granted access must read and sign an agreement acknowledging an understanding of the person's responsibilities for password security and maintaining the confidentiality of the data that he/she accesses. The signed agreement is kept on file in the Information Technology Department and the Human Resources Department.

What happens when an employee terminates employment? The supervisor is responsible for maintaining the overall security of the access and release of information in his/her department. When a staff member terminates employment or transfers to another department, access must be removed or revised. In order to initiate access deletion or revision, the supervisor must notify Human Resources of such changes. A new request for access must be submitted for a personnel replacement.

What happens if a security violation is detected? The employee should immediately change his/her password, or have Information Technology Department reset it, and notify the supervisor.

Who does an employee contact with questions about access? The first contact should be with the supervisor. Questions regarding assistance with computer equipment and hook-up should be directed to the Information Technology Department. Also, if an authorized access user has forgotten his/her password, the person should contact Information Technology Department at ext. 6725 or 6732.

RELEASE OF STUDENT INFORMATION POLICY

East Central College will comply with all state and federal statutes regarding use and release of student information including the Family Educational Rights and Privacy Act of 1974 (FERPA)(as amended). Students, parents or guardians seeking clarifications of laws, regulations and practices may request such information from the Vice President, Student Affairs office.

Cc: IT Department