

**ARC 605**

Digital Student Data Transfer Policy

**PURPOSE**

Establishes the policy and expectations for transferring student data-sets electronically internally or externally.

**SUMMARY**

Student data typically includes sensitive and confidential information that should not be shared unless it is being shared as part of a legitimate educational interest. Breaches of student information could result in harm to individuals, financial loss, damage to the person’s reputation, or legal repercussions. Maintaining the integrity of our student records to ensure information is not accessed and distributed by unauthorized individuals is every employee's responsibility.

Employees must use privacy and security best practices when sharing student records. Unencrypted methods of data transfer, such as email, should not be used for transferring electronic datasets for more than a few students.

Sharing data using allowable encrypted methods are outlined in ARC 605P.

**DEFINITIONS**

“A few students” are defined as 5 or less and would have the lowest amount of impact and harm in the case of a data breach. Allowing the use of email for a few students will reduce the impact on day-to-day processes.

“Student data” is defined as anything related to the student, including contact, demographic, and all academic information.

**EXCEPTIONS**

1. Situations where information is being shared directly with the student and the student’s identity has been verified (contact Registrar for proper protocols)
2. Fulfilling subpoenas.

**Applicability**

This policy applies to all College employees.

**Enforcement**

In the event of a data breach, the appropriate CCC employee will work with the Registrar and appropriate authorities to take the following actions:

* Determine what information was compromised.
* Take immediate steps to retrieve data and prevent further disclosures.
* Identify which policies and procedures may have been breached.
* Identify all affected records and students.
* Report to legal authorities.
* Connect with responsible parties and clarify oversight and accountability.
* Risk assessment of further breaches.
* Notify students of the breach and remediation options.
* The Registrar is required to make a note on the student record.

**RELATED**

Current CCC [FERPA policy](https://www.clackamas.edu/docs/default-source/about-us/accreditation-and-policies/ccc-ferpa-policy.pdf?sfvrsn=919479b9_0) and CCC Board of Education policy on [directory information](https://policy.osba.org/clackcc/J/JOA%20G1.PDF)

**EFFECTIVE DATE:**

This policy goes into effect upon approval.

**END OF POLICY**

**APPROVALS**

|  |  |
| --- | --- |
| Last Reviewed and Updated |  |
| Maintained By | Access, Retention, and Completion Committee (ARC) |
| Administered By |  |
| ARC Initial Review |  |
| ISP Committee – if appropriate |  |
| College Council – first reading |  |
| College Council – second reading |  |
| President’s Council – if appropriate |  |
| Final ARC Review and Approval |  |