# STUDENT AND THIRD-PARTY PHONE AUTHENTICATION POLICY

*Student Services*

## Publicly Shared Information

### *Policy Statement*

To ensure compliance with the Family Educational Rights and Privacy Act (FERPA) and to protect the confidentiality of student records, all staff must follow strict procedures when authenticating the identity of a student or an authorized third party over the phone.

### *Policy Details*

**No confidential information** (including non-directory information) may be disclosed unless the caller's identity is properly authenticated.

**Social Security Numbers and Dates of Birth** should not be used for authentication purposes. They may, however, be used to find the student in the Student Information System (SIS).

If a student has a **Directory Hold** on their record, no information may be released to any third parties without a documented FERPA Release.

When in doubt, **do not disclose** any information and refer the caller to the appropriate office for in-person verification.

### *Procedures*

### *Authentication Process*

#### For Active Students:

Staff must ask at least three of the following questions. All must be answered correctly:

- Student ID number or institutional username
- Current mailing or permanent address on file
- Personal email address on file
- Program of study (major)
- One course currently enrolled in (or recent past term)
- Entry term or anticipated graduation date
- Name of a current instructor, or recent instructor if not currently enrolled

#### For Former Students:

Ask three of the following:

- Student ID number
- Last mailing address on record
- Personal email address on file
- Last term or year of attendance
- Program of study (major)

- One course previously completed
- Name of a former instructor

### For Authorized Third Parties:

Verify that a FERPA Release is on file (SPACMNT)

- Note what information may be disclosed and to whom.
- Verify Expiration Date has not passed
- Confirm the identity of the third-party using the **name** and **passphrase**
- Only share information explicitly authorized in the release.

### If Authentication Fails:

- Do not release any information.
- Advise the caller to visit the appropriate office in person with a valid photo ID.
- Document the interaction if necessary and notify a supervisor.

## *Resources*

U.S. Department of Education – Identity Authentication Best Practices - Privacy Technical Assistance Center (PTAC) provides FERPA-compliant recommendations for authenticating students and third parties.

## Documentation

## Definitions

| *Term* | **Definition** |
|---|---|
| | |
| | |

## *Approval History*

| *Date* | Policy/Procedure or Entire Document | Notes (Types of Actions) | **Approved by |
|---|---|---|---|
| 10/23/2025 | Policy | New | CASA Co-Chair, Dr. Doug Mead |
| | | | |
| | | | |

**Full name of CASA Committee Chair, signatory, or designee

**Effective Date: 10/24/2025**

**Next Review Date: 10/31/2026**