UMPQUA COMMUNITY COLLEGE

Umpqua Community College transforms lives and enriches communities.

Work Session - 3:30 P.M., HNSC 101:
Industrial Technology Center Plans and UCC Facilities Assessment Report
Jess Miller, Director of Facilities & Security

VOL. LIV, No. 8 BOARD OF EDUCATION MEETING

March 11, 2019; 4:30 P.M., HNSC 101

Executive Session per ORS 192.660(2)(d)
Following the meeting; HNSC 101

AGENDA

MEMBERS:				ADMINISTRATION:	
Steve Loosley, Chair	____	Randy Richardson	____	Debra Thatcher	____
Guy Kennerly, V. Chair	____	Erica Mills	____	Kacy Crabtree	____
Doris Lathrop	____	Twila McDonald	____		
David Littlejohn	____				

I. CALL TO ORDER — **Chair Loosley**

II. ATTENDANCE — **Chair Loosley**

III. PLEDGE OF ALLEGIANCE — **Chair Loosley**

IV. CITIZEN COMMENTS

The Board values inputs from citizens of the Umpqua Community College District. Citizens wishing to speak shall sign-in on the Public Comment sheet prior to the start of the meeting. At the time specified on the agenda, the citizen shall state their name, address, and city of residence. Comments will be limited to three to five minutes, at the discretion of the Board Chair. The Board may not respond directly to any issues raised but refer those issues to the President for appropriate action.

V. CONSENT AGENDA — **Chair Loosley** — **pp 1-151**

All matters listed under Consent Agenda are considered by the Board of Directors to be routine or sufficiently supported by information as to not require additional discussion. Consent Agenda items will be enacted by one motion. There will be no separate discussion of these items prior to the time the Board votes on them, unless a Board member requests a specific item be removed from the Consent Agenda for discussion and a separate vote.

VI. CHANGES TO THE AGENDA — **Chair Loosley**

VII.	**REPORTS**		**p 152**
	A. Standing Reports		
	1. ASUCC Report	**Jesika Barnes**	
	2. ACEUCC Report	**Susan Neeman**	
	3. UCCFA Report	**John Blackwood**	
	4. UCCPTFA Report	**Jenny Friedman**	
	5. OCCA Report	**Doris Lathrop**	
	6. President's Report	**Debra Thatcher, President**	
	7. Chair's Report	**Chair Loosley**	
	B. Informational Reports ***(written reports submitted, no discussion)***		**pp 153-166**
	1. Accreditation Update ***(standing)***	**Debra Thatcher**	
	2. Advancement Update	**Tiffany Coleman**	
	3. Winter 2020 Enrollment Report	**Missy Olson**	
VIII.	**OLD BUSINESS**		
IX.	**NEW BUSINESS**		
	A. First Reading of Policies	**Debra Thatcher**	**pp 167-210**
	B. Discussion of Bond for Capital Improvements	**Chair Loosley**	**p 211**
X.	**BOARD COMMENTS**	**Chair Loosley**	
XI.	**ADJOURNMENT**	**Chair Loosley**	

NEXT BOARD MEETING:

- Board Meeting, April 8, 2020, 4:30 pm, HNSC 100

Robynne Wilgus, Board Assistant, 541-440-4622 voice, Oregon Relay TTY: 711. The UCC Board will provide, upon request, reasonable accommodation during Board meetings for individuals with disabilities.

BOARD OF EDUCATION
UMPQUA COMMUNITY COLLEGE
DOUGLAS COUNTY, OREGON

____ Information Item

_X_ Action Item

Subject: Consent Agenda (3 pages)

Date: March 11, 2020

Recommend approval of:

1. Minutes of College Board Meeting of February 12, 2020 — pp 1-3
2. Minutes of College Special Board Meeting of February 26, 2020 — pp 4-5
3. Personnel Actions — p 6
4. The following policies are coming to the Board for a second reading: — pp 7-101

Old #	New #	Title
600.4	3310	Records, Retention and Destruction
404	3440	Animals on Campus
N/A	5200	Student Health Services (No AP)
N/A	5210	Communicable Disease – Students
N/A	5400	Associated Students Organization
N/A	5410	Associated Students Elections
N/A	5420	Associated Students Finance
740	5610	Voter Registration & Information
600.05	6300	Fiscal Management
N/A	6316	Debt Issuance and Management
601	6330	Purchasing

The associated administrative procedures are being shared as an information item:

Old #	New #	Title
N/A	3310	Records, Retention and Destruction
404	3440	Animals on Campus
N/A	5210	Communicable Disease – Students
N/A	5400	Associated Students Organization
N/A	5410	Associated Students Elections
N/A	5420	Associated Students Finance
740	5610	Voter Registration & Information
600.05	6300	Fiscal Management
N/A	6316	Tax-Exempt Compliance
601	6330	Purchasing
601.1	6331	Credit Card Use
319.03 BP/AP	7345	Vacation Leave for Administrative / Confidential-Exempt

Recommendation by:

Raynne Wilgus

Approved for Consideration:

Debra Thatcher

BOARD OF EDUCATION
UMPQUA COMMUNITY COLLEGE
DOUGLAS COUNTY, OREGON

___ Information Item

_X__ Action Item

Subject: Consent Agenda, page 2
Second Reading of Board Policies

Date: March 11, 2020

The following policies are coming to the Board for a second reading:

OLD	NEW	TITLE	Pages 102-149
100	2000	Organization and Authority	
100.01	2010	Board of Education Membership	
100.03	2100	Board of Education Elections	
100.05	2110	Vacancies on the Board of Education	
100.05	2110AP	Vacancies on the Board of Education	
100.1	2200	Board of Education Duties and Responsibilities	
100.04, .11, .12, .13	2210	Board of Education Officers	
100.06	2220	Committees of the Board of Education	
N/A	2305	Board of Education Annual Organizational Meeting	
103	2310	Regular Meetings of the Board of Education	
103.01	2310AP	Regular Meetings	
103.02	2315	Closed Executive Sessions	
103.03	2320	Special Meetings	
103.03, .04	2320AP	Special and Emergency Meetings	
103AP	2330	Quorum and Voting	
103.05	2340	Agendas	
103.05AP	2345	Public Participation at Board of Education Meetings	
103AP	2350	Speakers	
103AP	2355	Decorum	
103.06	2360	Minutes	
101, 101.01, 102	2410	Board Policies and Administrative Procedures	
100.07, 14	2430	Delegation of Authority to the President	
N/A	2431	Selection of the President	
N/A	2432	~~Succession~~ Designation of Acting President	
N/A	2435	Evaluation of the President	
N/A	2610	Presentation of Initial Collective Bargaining Proposals	
N/A	2610AP	Presentation of Initial Collective Bargaining Proposals	
104	2710	Conflict of Interest	
104	2710AP	Conflict of Interest	
100.08	2715	Code of Ethics / Standards of Practice	
N/A	2716	Board of Education Political Activity	
N/A	2717	Personal Use of Public Resources - Board of Education	
100.07	2720	Communications Among Board of Education Members	
100.09	2725	Board of Education Member Compensation	
N/A	2735	Board of Education Member Travel	
100.17	2745	Board of Education Self Evaluation	
107	2800	Separation of College and Foundation	

Recommendation by:

Approved for Consideration:

Debra Thatcher

BOARD OF EDUCATION **UMPQUA COMMUNITY COLLEGE** **DOUGLAS COUNTY, OREGON**	____ Information Item _X_ Action Item
Subject: Consent Agenda, page 3 Policies to be deleted	Date: March 11, 2020

The following policies are coming to the Board for a second reading for deletion:

#	**Title**	**Pages # 150-151**
100.15	Legal Counsel	
106	Association Memberships	

See separate Consent Agenda packet (pages 1-151) for the related documents.

Recommendation by:	Approved for Consideration: Debra Thatcher

BOARD OF EDUCATION
UMPQUA COMMUNITY COLLEGE
DOUGLAS COUNTY, OREGON

__X__ Information Item

____ Action Item

Subject: Standing Reports

Date: March 11, 2020

ASUCC Report	Jesika Barnes
ACEUCC Report	Susan Neeman
UCCFA Report	John Blackwood
UCCPTFA Report	Jenny Friedman
President's Report	Debra Thatcher, President
OCCA Report	Doris Lathrop
Chair Report	Steve Loosley

Recommendation by:

Approved for Consideration:

Debra Thatcher

BOARD OF EDUCATION **UMPQUA COMMUNITY COLLEGE** **DOUGLAS COUNTY, OREGON**	__X__ Information Item ____ Action Item
Subject: Informational Reports	Date: March 11, 2020

Accreditation Update	Debra Thatcher
Advancement Update	Tiffany Coleman
Winter 2020 Enrollment Report	Missy Olson

Recommendation by:	Approved for Consideration: Debra Thatcher

Overview

In the 2019-20 Academic Year, UCC is addressing a set of core accreditation requirements, led by the Division of Institutional Effectiveness, the Senior Leadership Team, and Provost Council. Requirements include academic assessment; systematic and data-informed decision-making; and an effective governance system. Progress in academic assessment work is on track.

Student Learning Assessment - *UCC faculty and administration must collaboratively develop and implement a systematic approach to assessing student learning.*

Status: ***On Track***
In January, all faculty completed academic assessment work from Fall term on student learning outcomes. The Academic and Curriculum Assessment Committee (ACSC) is currently reviewing the assessments and will be providing feedback to faculty before the end of Winter term. ACSC continues to work with faculty to provide input on incorporating assessment and curriculum strategies and procedures.

In January, The Division of Institutional Effectiveness completed an initial round of data packets on academic programs, in draft form. These packets are formatted to provide data on enrollment, retention, and student success. They will be introduced to campus in Spring term for stakeholder review, and then will be used in June for each academic area to complete academic program assessments.

Next Steps:

- ACSC will complete feedback on student learning outcomes and provide to all faculty.
- ACSC will plan for Spring In Service, including re-introducing the annual academic program assessment process, which will incorporate data provided by IR.
- Faculty and the Division of IE will work to introduce academic program data to campus for stakeholder review, and then use during the In Service days at the end of the academic year.

Data-Informed Decision-Making - *UCC must implement an institution-wide system of data-informed evaluation and planning to guide institutional decisions, continuous improvement, resource allocation, and measurements of institutional effectiveness.*

Status: ***On Track***
Work continues in the areas of Institutional Effectiveness across UCC. To meet accreditation requirements, UCC must demonstrate that it is collecting and using data across all areas of operation to guide decision-making and improve institutional effectiveness.

UCC has completed its 2020-2021 Strategic Resource Request process, which included a ranking process for funding requests designed to address strategic prioritization and impact on college operations and student success. The Senior Leadership Team has announced funding decisions and a report on the process, which is now available on the Business Office website for review.

Additionally, each Tactical area completed mid-year assessment plans. These were collected by the Division of IE and compiled at the Strategic Level to provide reporting on Strategic Plan progress. The Strategic Plan Oversight Committee will meet on March 10th to review progress and provide analysis at the Strategic Goal level. This will be used to produce a final Strategic Plan Mid Year Progress report document. IE is currently working on providing Institutional Indicator data, which will be incorporated into analysis on progress and next steps for the end of year Strategic Plan Report.

Institutional Indicators will be distributed for review by April 1. These institutional indicators will be used for analysis of the Strategic Plan report. They will also be posted publicly to meet the new NWCCU requirements that data is used and made public.

Governance - *UCC must increase institutional stability through effective leadership and governance processes.*

Status: On Track

All governance councils have a web page to publish their charter, their membership, and their meeting notes. Each council was asked to update their web page to include each term's meeting schedule, publish a meeting agenda, provide a meeting summary to Umpqua Updates, update their charter to include “advisory” in each name, and update their charter to change any reference to “decision-making” to “recommendations and/or proposals”.

Most governance councils have updated their information page with the additional information required. Providing an agenda three days before a scheduled meeting has proven challenging depending on the meeting schedule since some councils meet more often than others and this guideline is under review. Charters have been updated winter term 2020 to comply with the guidelines.

Conclusion

All areas across UCC are aware of UCC’s accreditation status and are contributing to the development and implementation of processes crucial to meeting accreditation requirements. Related campus training will continue to be ongoing and supported. Academic assessment continues to be a challenge due to the heavy educational lift. Reports on the deliverables stated in this report, and any others that are created to meet requirements, will continue to be provided to the Board on a monthly basis.

Academic Assessment Deliverables and Compliance, through 12/6/2019

Who	Deliverable	Due	Compliance
All Chairs/Program Coordinators	Detailed Year Timeline	10.4.19	31/33 (93.4%)
Chairs/Program Coordinators	Curriculum Maps and Questionnaire	10.4.19	29/33 (87.9%)
A&S Chairs	Courses identified to assess AAOT PLOs	10.4.19	Completed as a division
All Chairs/Program Coordinators	CLO/PLO/ULO Assessment Assignments (who is doing what form this term)	10.4.19	31/33 (93.4%)
Chairs/Program Coordinators with CTE programs	Program Update Form	10.15.19	80/84 (94%)
AAOT Chairs	Rubrics for PLOs	11.15.19*	4/4 (100%)
CTE Chairs/Program Coordinators	Rubrics for PLOs	11.15.19*	20/33 (60%)
All Faculty	CLO/PLO/ULO Assessments	1.17.19	N/A

* Previous dates were 11.11.19, but were shifted forward due to Veterans Day on 11.11.19

	Indicator		Indicator Description
1	Retention	Part 1: % of PT and FT UCC degree and certificate-seeking students are retained fall-fall; Part 2: % persist fall to winter	Part 1: How many students return from one fall to the next, PT and FT ; Part 2: How many students return in winter term who were enrolled in fall term, PT and FT - excluding those students who graduated
2	Early Momentum	% of students who complete based on # of credits they complete within their first terms	Rates at which 1st time students complete 18+ college level credits in their first year
3	Graduation	% of entering degree/certificate students who complete a degree/certificate within 3 and 6 years	How many students who seek degrees or certificates complete a degree or certificate within 3 and 6 years, as determined by their Banner code "program" of declaration.
4	Transfer	% of students who transfer to another institution within one year of most recent UCC enrollment within the past 3 years (reported by: Students who have received a credential, and those who did not.)	Number of students who transfer to their next institution within one year of enrollment at UCC.
5	Program-level Learning Outcomes:	% of Program Learning Outcomes are achieved at or above "proficient" levels.	PLO assessments each year demonstrate that at least 80% of students have reached a "proficient" level of that program competency. Proficiency is determined by each program.
6	Universal Learning Outcomes	% of degree/certificate-seeking students achieve ULO competencies at a "proficient" level.	ULO assessments demonstrate that at least 80% of degree/certificate-seeking students reach a "proficient" level of the ULO competency, as defined by a standardized ULO rubric. (certificates 45 credits and higher)
7	Student Success Rates	% of students pass what have been identified as a "gatekeeper courses"	Passing rate for gatekeeper courses.

8	Academic and Student Support Services	% of all areas of operation that identify and implement next steps for improvement as a result of programmatic assessment.	All areas of operation will assess, identify next steps, and implement them for improvement. This measurement will demonstrate whether or not assessment processes are occurring.
9	Equitable Outcomes	Statistically significant equity gaps identified in Transfer, Graduation, and Retention/Persistence, course pass rates decrease annually between: *Male/Female students, students of color and white students, athletes/non-athletes, students who use accessibility services and those who do not, students who are Pell eligible versus non-eligible, veterans versus non-veterans*	Identified equity gaps will be measured as a lagging indicator for equitable outcomes of ongoing student success efforts.
10	Admissions Yield Rate	% of students who apply for UCC admissions will be enrolled within one year.	Yield rate of admissions applications.
11	Life-long learning opportunities	Ability to meet community needs, measured by: ABS: Enrollment based on % of pop without a GED and GED completion rates CWT: Repeat rates of community members attending CWT community courses SBDC: Rate of meeting established impact benchmarks by quarter.	Ability to meet community needs by indicators specific to areas of operation.
12	Campus/Community Engagement	Community, students, and staff satisfaction ratings for any area of operation that received less than 70% "satisfied" responses demonstrates an increase in satisfaction rating in the next survey (done every 3 years).	Satisfaction rate for UCC services with less than 70% satisfaction rate increases.
13	Student Experience	% of UCC students who believe that their experience at UCC has contributed to their knowledge, skills and personal development	Students who believe their experience at UCC contributed to their knowledge, skills, and personal development.

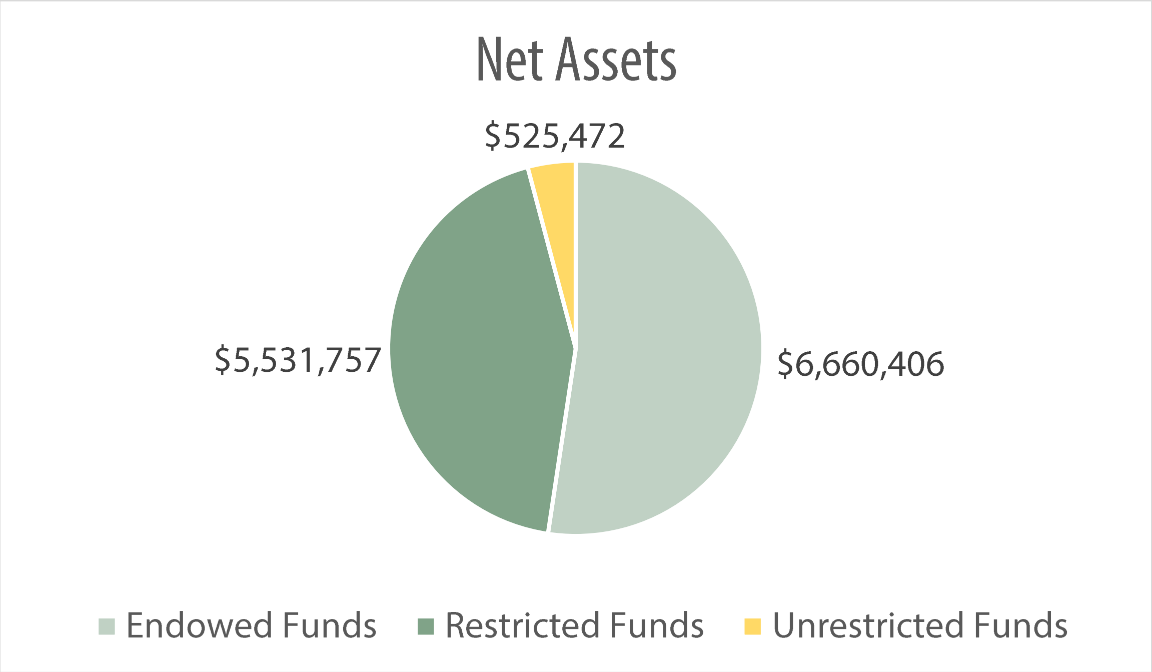
Actions to be taken by all Governance Councils

Changes required by November 15th, 2019

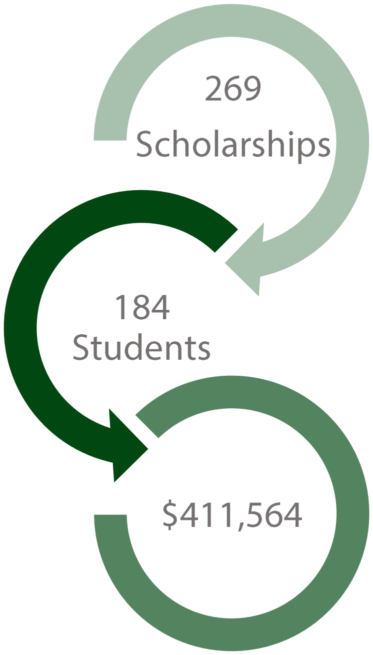
NAME	All governance councils are to include “Advisory” in their titles
MEETINGS	At the beginning of each term, publish the meeting dates for the entire term on MyUCC in the respective areas for your councils.
	Publish the agenda of council meetings 3 days in advance on Umpqua Updates, notifying people of topics to be discussed and inviting any interested persons to attend the meetings. The purpose of these two actions is to encourage greater participation in governance.
NOTES / MINUTES	All meeting notes are to be published to the governance section of MyUCC. This year, in an effort to get more people to read the notes, the following changes are needed:
	Preface each set of minutes with a 2-3 sentence summary of actions or key discussions before posting to the intranet.
	Submit these summaries to Umpqua Updates after each meeting as soon as your notes are posted. The hope is that the summary in Umpqua Updates will inform people, encourage them to go to the intranet and read more, and perhaps even decide to attend meetings or join a council.
CHARTER	Change the section in your charter entitled, “Decision Making/Recommendations” to “Recommendations and Proposals” and remove any language throughout the charter that refers to making decisions, replacing it with making recommendations/proposals. The change in language does not remove the importance of the work of councils; instead, it clarifies the role of governance bodies as those that advise.
	Review your charter for clarity regarding purpose and process. If you have questions about purpose, process, or any other area of the charter, contact College Council by **October 28**. (Send inquires by email to Robynne.) Update the charters, if necessary, to clarify purpose and process.
	Submit your updated charter with change in name, advisory role, purpose, process, etc. to the College Council by **November 15.** (Send documents by email to Robynne.)
GOALS	Each charter should identify 1 to 3 goals for the year. Send your goals to College Council by **November 15.** (Send via email to Robynne.) The goals should be measurable and be connected to the strategic plan. You will be asked to report your progress at least once during the year and again at the end of the year.

UCC
UMPQUA COMMUNITY COLLEGE
FOUNDATION

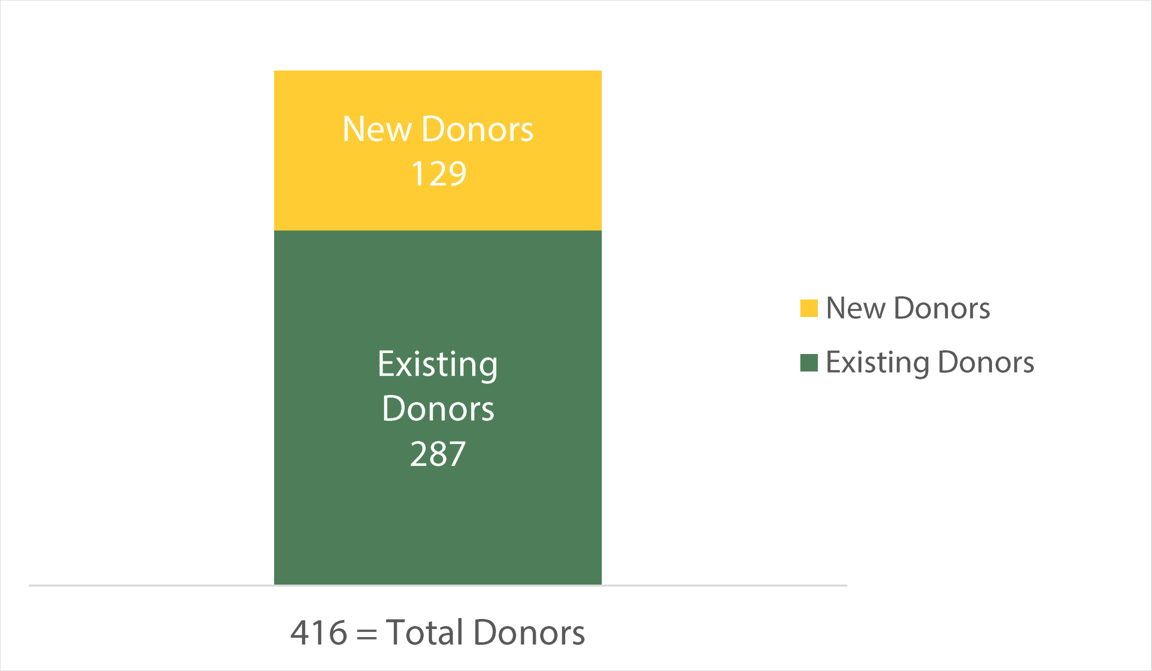
2019 Annual Report



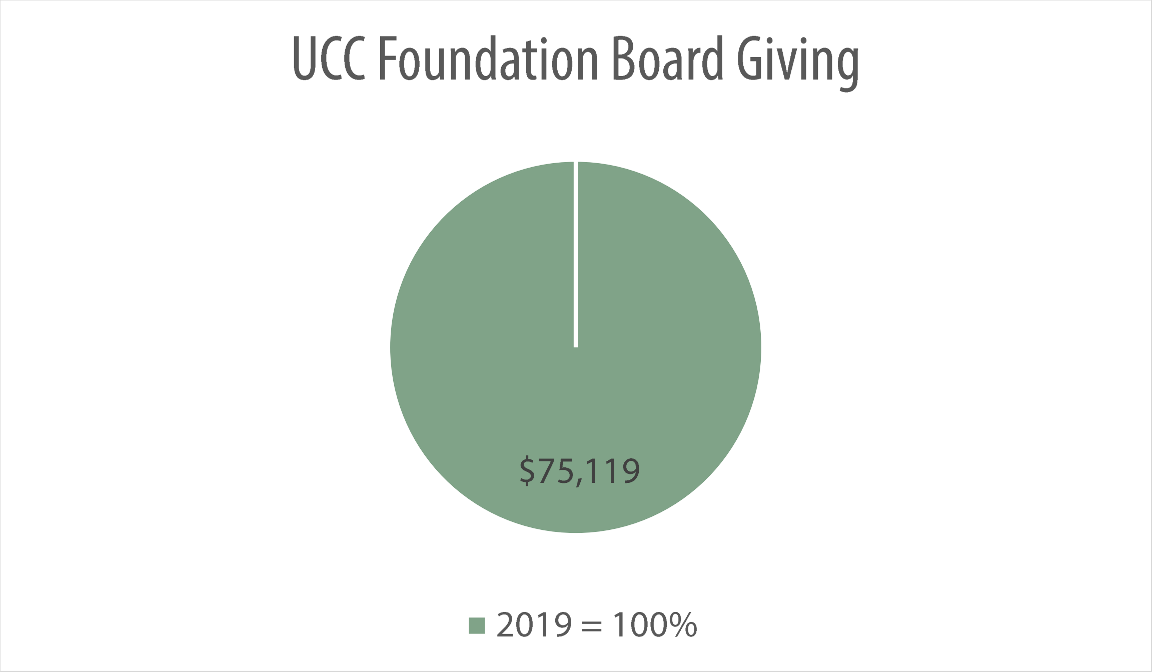
This report is based on the 2019 calendar year (January 1 through December 31). In 2019, the UCC Foundation's net assets equaled $12,717,635.



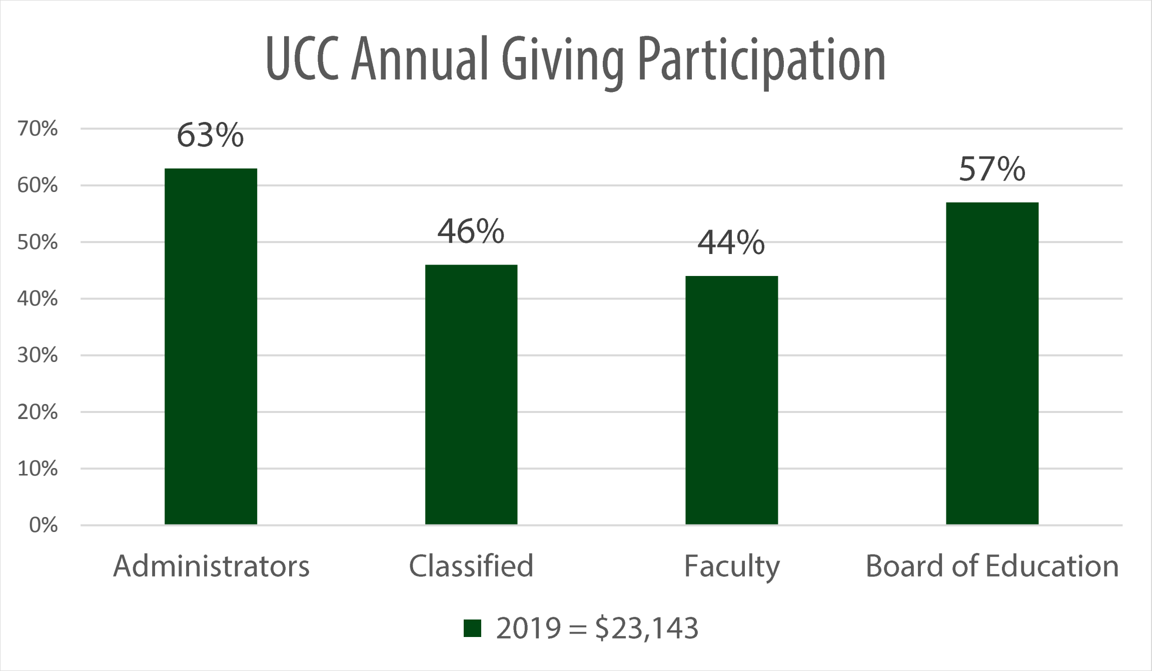
This year, the UCC Foundation awarded 269 scholarships to 184 students totaling $411,564.



In 2019, a total of 416 donors gave more than $771,000. Of the total donor base, 129 were new donors this year.

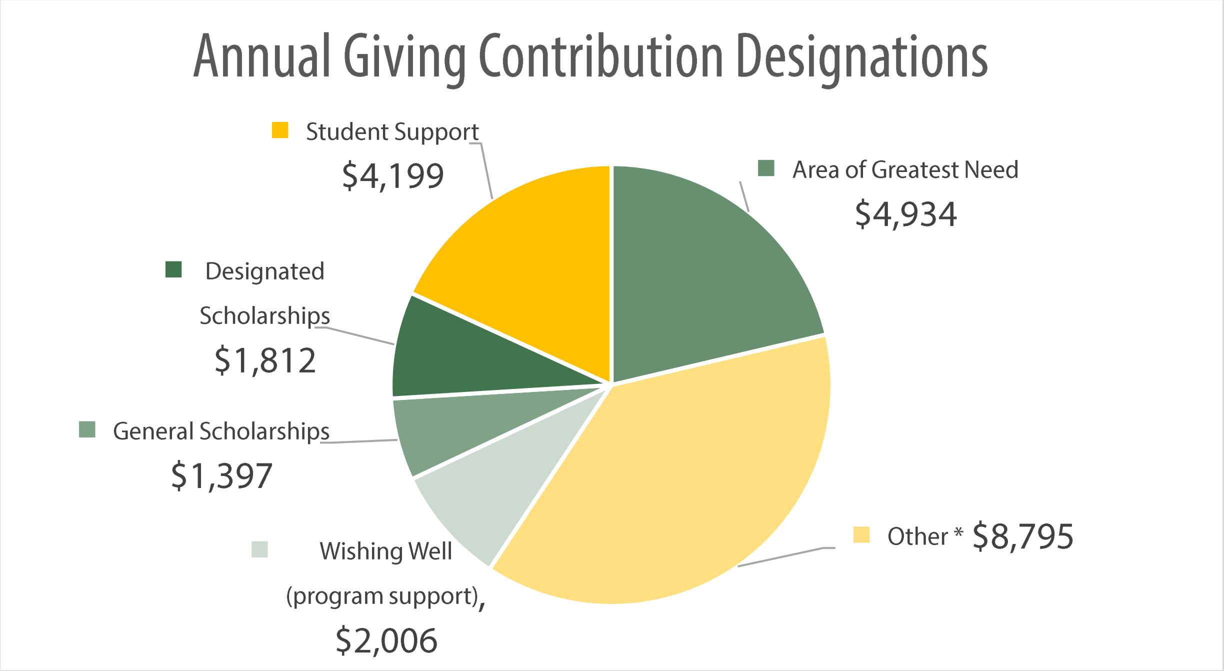


The UCC Foundation's 35-member, all-volunteer Board gave more than $75,000 in financial contributions. The average monetary contribution per Board member = $2,146. The total includes all contributions associated with the Legacy Ball and any annual giving initiatives.



In 2019, 105 people—consisting of administrators, classified staff, faculty, and the Board of Education—contributed $23,143 to UCC's Annual Giving Campaign. Of those participating:

26 of 41	Administrators
47 of 102	Classified Staff
28 of 63	Faculty
4 of 7	Board of Education



*Other includes: Paralegal, Legacy Ball, Paul Morgan Observatory, 10/1 Memorial, Educational Talent Search (ETS)/Upward Bound (UB), Athletics, Transfer Opportunity Program (TOP), Industrial Arts Technology Building.

Winter 2020 Enrollment Report

Missy Olson, Dean of Enrollment Management
February 24, 2020

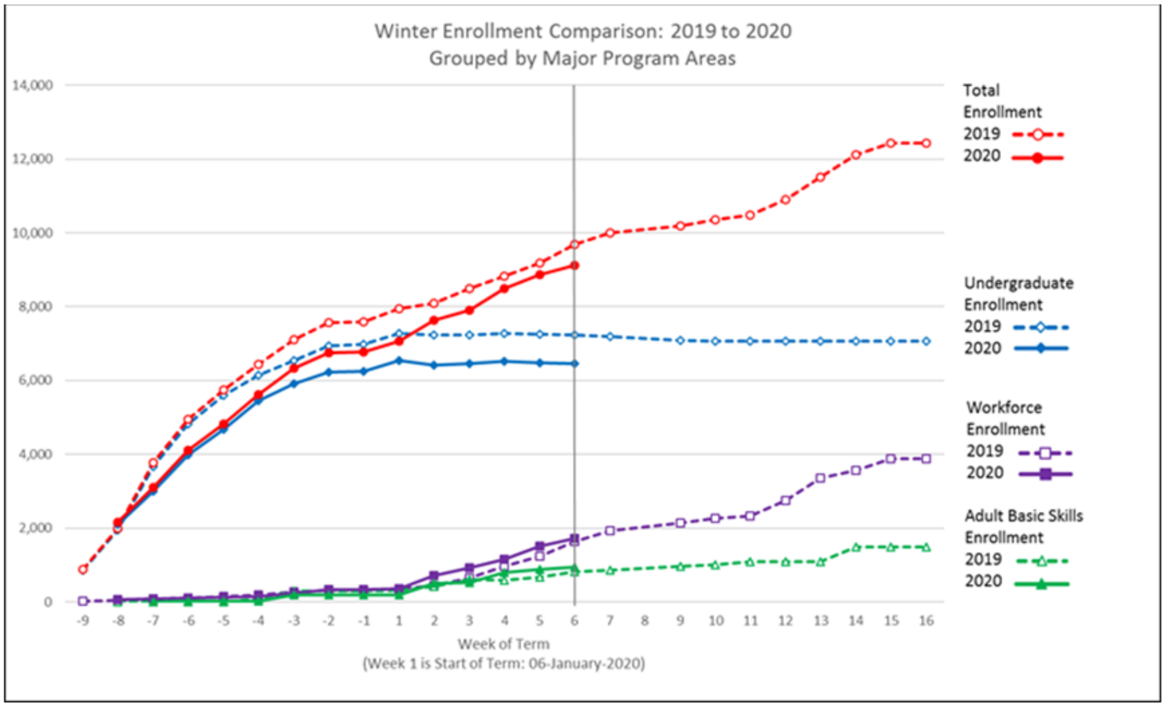
Overall Trends-Winter Term

- ABS is trending up, mainly due to increased educational requirements at Wolf Creek Job Corps
- Dual credit enrollment is down
- Community and Workforce Training (CWT) registrations come in throughout the term

Data Sources:

- FTE data comes from Institutional Research regular enrollment reports
- Enrollment Management tracks Admissions to Enrollment yield and current term enrollment by student declared major. Data is from Banner.

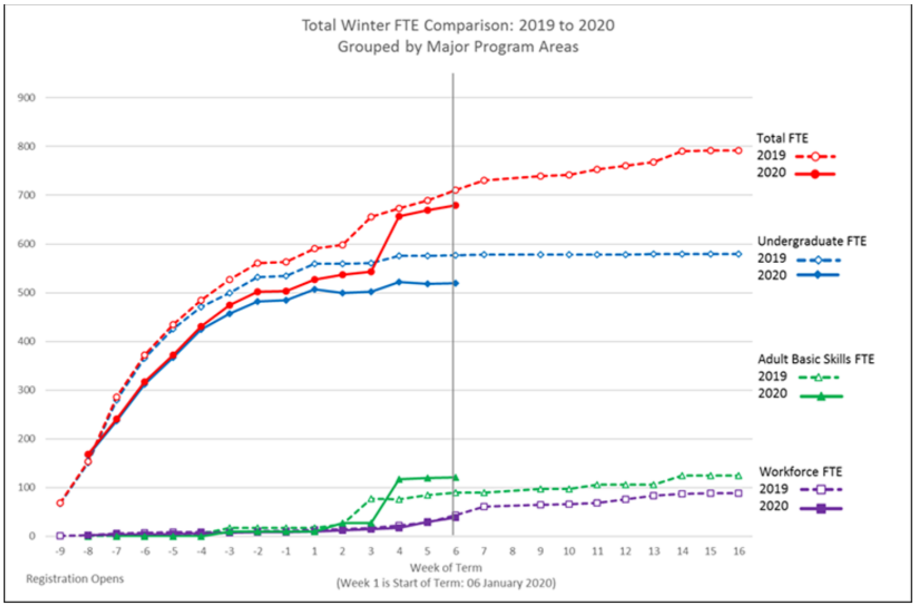
Enrollment



Winter Credit Enrollment Trends

House	Area	Winter 2018			Winter 2019			Winter 2020		
		Total Enrollment (Student Declared)	Admissions applications for term (Overall Interest)	Converted Admissions (in same term)	**Total Enrollment (Student Declared)**	Admissions applications for term (Overall Interest)	Converted Admissions (in same term)	**Total Enrollment (Student Declared)**	Admissions applications for term (Overall Interest)	Converted Admissions (in same term)
Other	AAOT/AGS/Non-Degree	**761**	216	94	**665**	179	89	**604**	182	68
Humanities	Public Relations	**0**	1	0	**0**	0	0	**0**	1	0
Arts	Music SOU	**4**	0	0	**5**	1	0	**6**	0	0
Science/Math	Natural Resources	**8**	1	0	**10**	5	2	**13**	1	0
Social and Behavioral Sciences	Early Childhood Ed	**25**	6	2	**28**	18	8	**33**	13	4
	Human Services	**56**	36	11	**73**	36	17	**64**	28	8
	Paralegal	**34**	11	6	**44**	22	9	**52**	20	10
Applied Science and Technology	Automotive	**21**	15	4	**29**	14	3	**25**	10	3
	Computers	**73**	48	22	**65**	23	9	**50**	15	7
	Engineering	**47**	21	10	**44**	12	5	**45**	13	7
	Apprenticeship	**63**	18	9	**65**	22	16	**127**	9	6
	Welding	**31**	25	7	**35**	21	8	**29**	10	4
	Forestry	**22**	8	5	**25**	10	5	**20**	8	2
	Viticulture	**24**	9	2	**21**	9	4	**14**	9	2
Business	Business (w/o Retail)	**114**	76	25	**134**	56	16	**135**	37	11
	Retail Mgmt	**444**	95	77	**434**	118	96	**421**	89	57
Health	AAOT-pre-Nursing	**278**	109	38	**272**	69	27	**172**	74	17
	Nursing-accepted	**98**	6	3	**93**	3	1	**97**	1	1
	Dental Assistant	**31**	10	3	**28**	7	1	**20**	8	3
Public Safety	Criminal Justice	**58**	22	6	**73**	20	5	**46**	17	4
	Paramed/Fire Science	**63**	24	9	**66**	17	5	**70**	16	10
Dual Credit	Dual Credit	**441**	70	57	**479**	85	72	**386**	20	15
Ex. Options	Expanded Options	**150**	14	13	**108**	24	23	**132**	0	0

FTE



FTE			
Date of Report:	2/5/18	2/11/19	2/10/20
ABS	**94.58**	**89.03**	**120.89**
CWT	**6.87**	**22.36**	**15.92**
Transfer	**364.39**	**353.08**	**322.04**
Arts	13.26	15.49	14.31
Communications Studies	16.04	9.27	15.16
Early Childhood Education	1.53	3.11	3.58
Foreign languages	8.89	9.32	7.33
Health Human Performance	25.21	23.08	14.32
Human Services	8.99	11.58	9.32
Humanities	59.14	54.03	49.22
Learning Skills	5.29	8.85	5.93
Mathematics	79.67	67.88	62.2
Music	9.9	14.62	11.44
Physical Education	6.87	12.54	11.17
Science	71.46	68.89	67.16
Social Sciences	55.19	54.42	49.93
Theater Arts	2.95	0	.97
CTE	**201.29**	**240.79**	**208.45**
Apprenticeship	12.96	12.9	13.14
Auto	7.66	10.95	8.92
Business	70.56	86.98	75.33
Computer Science	22.56	16.85	14.99
Criminal Justice	7.76	7.83	6.88
Dental Assisting	9.55	11.32	5.41
Emergency Medical Services	8.58	14.48	8.74
Engineering	11.36	10.57	8.21
Fire Science	4.42	4.11	5.42
NA/Nursing	18.31	35.56	36.91
Paralegal	6.86	8.86	10.48
Viticulture	6.02	5.00	3.41
Welding	14.69	15.38	10.61
Other	**18.93**	**4.98**	**12.25**
Winter Totals	**686.06**	**710.24**	**679.55**

19-20 Strategies

- Developing and implementing retention plan
- Continuing the personalized onboarding outreach
- Starting review of class schedule for conflicts
- Supporting faculty work to enhance their programs and curriculum through enrollment status reports and prospective student interest
- Encouraging department specific outreach help, as it is very impactful
- Starting persistence/retention data review and campus-wide retention strategies
- Implementing additional recruitment strategies by target market

BOARD OF EDUCATION
UMPQUA COMMUNITY COLLEGE
DOUGLAS COUNTY, OREGON

_X_ Information Item

___ Action Item

Subject: First Reading of Policies

Date: March 11, 2020

The following policies are coming to the Board for a first reading:

Old #	**New #**	**Title**	**Pages**
N/A	4010	Academic Calendar	
344	4030	Academic Freedom	
N/A	4106	Nursing Programs	
600.08	5800	Prevention of Identity Theft in Student Financial Transactions	

The associated administrative procedures are being shared as an information item:

Old #	**New #**	**Title**
N/A	4010	Academic Calendar
344	4030	Academic Freedom
N/A	4106	Nursing Programs
600.08	5800	Prevention of Identity Theft in Student Financial Transactions

Recommendation by:

Approved for Consideration:

Debra Thatcher

UMPQUA COMMUNITY COLLEGE

BOARD POLICY

TITLE: Academic Calendar

BOARD POLICY # 4010

The Chief Academic Officer shall, in consultation with the appropriate groups and following the college-wide shared governance process, develop an academic calendar. The proposed calendar will be submitted to the Board of Education for approval.

RESPONSIBILITY:
The Chief Academic Officer is responsible for implementing and updating this policy. Specific guidance for policy implementation may be found in the associated Administrative Procedure(s).

NEXT REVIEW DATE:
DATE OF ADOPTION:
DATE(S) OF REVISION:
DATE(S) OF PRIOR REVIEW:

POLICY / ADMINISTRATIVE PROCEDURE CONVERSION TEMPLATE

Complete for Conversions Only

TITLE:	Academic Calendar		
New BP #:	4010	**Old BP # & Title:**	707 Academic Calendar
New AP #:		**Old AP # & Title:**	
Revision Date:	4/10/2019		

EXISTING POLICY / PROCEDURE	OCCA POLICY / PROCEDURE	PROPOSED POLICY / PROCEDURE
The Vice President of Instruction will establish an annual academic calendar in conjunction with a ~~college-wide shared governance process~~. After the calendar has been approved by the Board, it will be posted on the UCC website.	~~The~~ **[*CEO*]** ~~shall, in consultation with the appropriate groups,~~ **[*~~develop~~* or *submit to the Board of Education for approval*]** ~~an academic calendar.~~	The Chief Academic Officer shall, in consultation with the appropriate groups and following the college-wide shared governance process, develop an academic calendar. The proposed calendar will be submitted to the Board of Education for approval.

UMPQUA COMMUNITY COLLEGE

ADMINISTRATIVE PROCEDURE

TITLE: ACADEMIC CALENDAR
ADMINISTRATIVE PROCEDURE # 4010
RELATED TO POLICY # 4010 Academic Calendar

A. The College's three-year academic calendar shall include , at minimum, the following:

1. class registration
2. payment deadlines
3. dates classes begin and end each term (summer, fall, winter, and spring)
4. final examinations
5. last date to drop class(es) and be eligible for a refund as well as to add, withdraw, and/or change status from credit to audit
6. exceptions to the above for classes that meet for shorter periods during the term
7. college holidays, spring break, winter break, and campus closings
8. petition to graduate deadlines
9. Commencement

B. The academic calendar shall be of sufficient length to ensure the equivalent of 11 weeks of instruction per term (including final examination days) for all credit classes.

C. The Director of Registration and Records and the Chief Academic Officer will make reasonable efforts to coordinate the College's academic calendar with those of the public schools and regional institutions of higher education so that start dates and class breaks of any appreciable length (such as annual spring break) coincide in most systems.

D. After vetting through the appropriate College entities and approval by the College Board of Education for approval, the approved three-year calendar is published in the website. The UCC website will also post tentative academic calendars for the next two years.

RESPONSIBILITY:
The Chief Academic Officer is responsible for implementing and updating this procedure.

NEXT REVIEW DATE:	**DATE(S) OF REVISION:**
DATE OF ADOPTION:	**DATE(S) OF PRIOR REVIEW:**

POLICY / ADMINISTRATIVE PROCEDURE CONVERSION TEMPLATE

Complete for Conversions Only

TITLE:	Academic Calendar		
New BP #:		**Old BP # & Title:**	
New AP #:	4010	**Old AP # & Title:**	
Revision Date:	4/10/2019		

EXISTING POLICY / PROCEDURE	OCCA POLICY / PROCEDURE	PROPOSED POLICY / PROCEDURE
NA	• The number of days that define an academic year • Flexible calendar options, if any • Processes for determining the academic calendar • Holidays, which include: **[*insert*]** **Other Holidays** – The Board of Education may declare other days to be holidays and close the colleges and offices when good reason exists. **NOTE:** *These holidays may include New Year's Eve day, the day after Thanksgiving, and Christmas Eve day.*	The college's academic calendar shall include the dates of all operational activities that affect students and the public (such as registration dates and holidays during which the college is closed). These dates shall include, but not be limited to, the following: • class registration • graduation ceremony • midterm and final examinations • college holidays, and campus closings • petition to graduate deadlines • beginning and ending of summer, fall, winter, and spring quarters • return dates for full-time faculty • dates classes begin and end each term • last date to drop class(es) and be eligible for a refund as well as to add, withdraw, and/or change status from credit to audit • payment deadlines.

		The academic calendar should be of sufficient length to insure the equivalent of 11 weeks of instruction per term (including final examination days) for all credit classes. The Registrar and the Chief Academic Officer will make reasonable efforts to coordinate the college's academic calendar with that of the public schools and regional institutions of higher education so that start dates and class breaks of any appreciable length (such as annual spring break) coincide in most systems. After vetting through the appropriate UCC entities, the proposed academic calendar is submitted to the UCC board of education for approval, and the approved calendar is published in the college catalog, schedule and website. The UCC website will also post tentative academic calendars for the next two years.

UMPQUA COMMUNITY COLLEGE

BOARD POLICY

TITLE: Academic Freedom

BOARD POLICY # 4030 ***was 344 Academic Freedom***

Umpqua Community College is committed to the principle that institutions of higher learning benefit from academic freedom. Umpqua Community College defines academic freedom as the faculty's right to engage in intellectual debate, research, speech, writing, artistic expression, and all other forms of communication, both on and off campus, without fear of censorship or reprisal.

RESPONSIBILITY:
The Chief Academic Officer is responsible for implementing and updating this policy. Specific guidance for policy implementation may be found in the associated Administrative Procedure(s).

NEXT REVIEW DATE:
DATE OF ADOPTION:
DATE(S) OF REVISION:
DATE(S) OF PRIOR REVIEW:

POLICY / ADMINISTRATIVE PROCEDURE CONVERSION TEMPLATE

Complete for Conversions Only

TITLE:	Academic Freedom		
New BP #:	4030	**Old BP # & Title:**	344 Academic Freedom
New AP #:		**Old AP # & Title:**	
Revision Date:	4/10/2019		

EXISTING POLICY / PROCEDURE	OCCA POLICY / PROCEDURE	PROPOSED POLICY / PROCEDURE
~~Umpqua Community College is committed to the principle that institutions of higher learning benefit from academic freedom. Umpqua Community College defines academic freedom as the faculty's right to engage in intellectual debate, research, speech, writing, artistic expression, and all other forms of communication, both on and off campus, without fear of censorship or reprisal.~~	The **[entity**] shall support the principles of academic freedom, built upon the free expression and exchange of ideas that are inherent in the search for scholarly truth and upon which a free and democratic society depends. The College affirms the use of a variety of teaching methodologies to fulfill its obligation to raise difficult and meaningful questions in the educational development of students. Faculty members are entitled to freely discuss issues germane to their subject matter. This freedom involves the right to introduce controversial topics, as long as the manner of presentation involves objective reasoning and rational discussion. Academic freedom must be balanced with the obligation of the College to protect the right of students to learn in an environment characterized by civility, open inquiry, and	Umpqua Community College is committed to the principle that institutions of higher learning benefit from academic freedom. Umpqua Community College defines academic freedom as the faculty's right to engage in intellectual debate, research, speech, writing, artistic expression, and all other forms of communication, both on and off campus, without fear of censorship or reprisal.

	freedom from unlawful discrimination. While faculty have the right to present ideas and conclusions which they believe to be in accord with available evidence, they also have the responsibility to acknowledge the existence of different opinions and to respect the right of others to hold those views. Faculty and students have a responsibility to engage in teaching and learning that honors and respects divergent viewpoints that are grounded in cultures of reason, logic, evidence and responsible scholarship. When faculty (or any other College employees) speak or write as citizens, care should be taken to avoid the representation of any personal view as that of the **[entity].**	

UMPQUA COMMUNITY COLLEGE

ADMINISTRATIVE PROCEDURE

TITLE: Academic Freedom

ADMINISTRATIVE PROCEDURE # 4030

RELATED TO POLICY # 4030 Academic Freedom

Academic Freedom includes the following rights and responsibilities:

A. Faculty are entitled to freedom in the classroom in discussion and presentation of subject matter, both online and face-to-face. This includes the right to explore and discuss controversial issues and divergent points of view in relationship to the subject matters being discussed.

B. When speaking or writing as private individuals, faculty are entitled to exercise all rights of citizenship, as defined by and in accordance with decisions of the state and federal courts, and are free from institutional censorship or discipline. As scholars and educational officers, they should remember that the public may judge their profession and their institution by their statements. Therefore, in their written statements and at public speaking events, faculty should not state they are speaking for the institution.

C. Faculty are entitled to full freedom in intellectual inquiry and expression in terms of research, speech, writing, artistic endeavors, and all other forms of communication related to their discipline.

D. Any faculty who feels their rights have been violated in regards to Academic Freedom should refer to the grievance procedure outlined in their respective bargaining agreements.

References: NWCCU Standards 2.A.27 and 2.A.28; OAR 589-008-0100(f)

RESPONSIBILITY:
The Chief Academic Officer is responsible for implementing and updating this procedure.

NEXT REVIEW DATE:
DATE OF ADOPTION:
DATE(S) OF REVISION:
DATE(S) OF PRIOR REVIEW:

POLICY / ADMINISTRATIVE PROCEDURE CONVERSION TEMPLATE

Complete for Conversions Only

TITLE:	Academic Freedom		
New BP #:		**Old BP # & Title:**	
New AP #:	4030	**Old AP # & Title:**	344 AP Academic Freedom
Revision Date:	10/17/2019		

EXISTING POLICY / PROCEDURE	OCCA POLICY / PROCEDURE	PROPOSED POLICY / PROCEDURE
N/A	**References:** NWCCU Standards 2.A.27 and 2.A.28 OAR 589-008-0100(f) **NOTE:** *Although this policy is **recommended as good practice**, it is up to the entity to determine the applicability of this administrative procedure given state law and the entity's organizational culture. Local practice may be inserted here to implement board policy, if necessary.* NOTE: Oregon administrative rules address the formation of community college personnel policies by Boards of Education. OAR 589-008-0100(f) requires a statement regarding academic freedom and responsibilities. BP 4030 provides sample language and any additional language related to procedures may be added here.	Academic Freedom includes the following rights and responsibilities: A. Faculty are entitled to freedom in the classroom in discussion and presentation of subject matter, both online and face-to-face. This includes the right to explore and discuss controversial issues and divergent points of view in relationship to the subject matters being discussed. B. When speaking or writing as private individuals, faculty are entitled to exercise all rights of citizenship, as defined by and in accordance with decisions of the state and federal courts, and are free from institutional censorship or discipline. As scholars and educational officers, they should remember that the public may judge their profession and their institution by their statements. Therefore, in their written statements and at public speaking events, faculty should not state they are speaking for the institution. C. Faculty are entitled to full freedom in intellectual inquiry and expression in terms of research, speech, writing, artistic endeavors, and all other forms of communication related to their discipline.

		D. Any faculty who feels their rights have been violated in regards to Academic Freedom should refer to the grievance procedure outlined in their respective bargaining agreements.

UCC
UMPQUA COMMUNITY COLLEGE

BOARD POLICY

TITLE: Nursing Programs

BOARD POLICY # 4106

The UCC nursing programs will adhere to all applicable regulations, laws, and requirements located in Oregon ORS and OAR, as well as standards of all applicable accrediting or approval bodies, such as Oregon State Board of Nursing.

UCC nursing programs will maintain a detailed student code of conduct applicable to any student admitted to the nursing program. If a conflict exists with the UCC Student Code of Conduct, the nursing program code of conduct will prevail.

RESPONSIBILITY:
The Chief Academic Officer is responsible for implementing and updating this policy. Specific guidance for policy implementation may be found in the associated Administrative Procedure(s).

NEXT REVIEW DATE:
DATE OF ADOPTION:
DATE(S) OF REVISION:
DATE(S) OF PRIOR REVIEW:

UMPQUA COMMUNITY COLLEGE

ADMINISTRATIVE PROCEDURE

TITLE: Nursing Programs

ADMINISTRATIVE PROCEDURE # 4106

RELATED TO POLICY # 4106 Nursing Programs

A. The College's Associate Degree of Nursing (ADN) Program shall comply with relevant laws (ORS 678.010-678.445) and rules (OAR 851 Division 21) of the Oregon Nurse Practice Act.

B. Requirements of the relevant laws and rules include, but are not limited to:

1. Written program policies and procedures, congruent with those of the College, which are reviewed periodically.
2. Faculty responsibilities:
   a. Develop, implement and evaluate policies and standards for the advising, selection, admission, advanced placement, progression and graduation of nursing students within the framework of the policies of the College
   b. Develop, implement and evaluate policies for assessing student achievement in terms of course and program learning outcomes
   c. Evaluate student learning and performance, assign grades for courses according to policies, determine student progression within the program, and recommend successful candidates for the ADN degree
   d. Develop, implement and evaluate policies and procedures necessary for the operation of the ADN program
   e. Participate in review of the total nursing program
   f. Participate in determining academic policies and procedures of the College
   g. Provide mechanisms for student input into and/or participation in decisions related to the ADN Program
3. Written information for students regarding admission, readmission, transfer, progression, retention, dismissal and graduation requirements that are consistent with those of the College along with policies, procedures, and

processes specific to nursing students if justified by the nature and purposes of the ADN Program.

4. Biennial review of program policies and procedures to assure compliance with the OSBN Nurse Practice Act, Division 21 Rules.

C. The UCC ADN Policy Manual will be reviewed every two years.

D. The UCC ADN Student Procedures Handbook will be reviewed annually (each spring term).

References
ORS 678.010-678.445 Oregon Nurse Practice Act
OAR 851

RESPONSIBILITY:
The Chief Academic Officer, in conjunction with the Director of Nursing, is responsible for implementing and updating this procedure.

NEXT REVIEW DATE:
DATE OF ADOPTION:
DATE(S) OF REVISION:
DATE(S) OF PRIOR REVIEW:

UMPQUA COMMUNITY COLLEGE

BOARD POLICY

TITLE: PREVENTION OF IDENTITY THEFT IN STUDENT FINANCIAL TRANSACTIONS

BOARD POLICY # 5800 ***(was 600.08 Identity Theft Prevention)***

The College is required to provide for the identification, detection, and response to patterns, practices, or specific activities (“Red Flags”) that could indicate identity theft of students when the College serves as a creditor in relation to its students. When applicable, the Chief Financial Officer is directed to develop procedures to implement an Identity Theft Prevention Program (ITPP) to control reasonably foreseeable risks to students from identity theft.

References:

15 U.S. Code Section 1681m(e), (Fair and Accurate Credit Transactions Act)

ORS 646A.600 to 646A.628 (Oregon Consumer Identity Theft Protection Act)

RESPONSIBILITY:
The Chief Financial Officer is responsible for implementing and updating this policy. Specific guidance for policy implementation may be found in the associated Administrative Procedure(s).

NEXT REVIEW DATE:
DATE OF ADOPTION:
DATE(S) OF REVISION:
DATE(S) OF PRIOR REVIEW:

POLICY / ADMINISTRATIVE PROCEDURE CONVERSION TEMPLATE

Complete for Conversions Only

TITLE: Prevention of Identity Theft in Student Financial Transactions

New BP #: 5800 **Old BP # & Title:** 600.08 Identity Theft Prevention

New AP #: **Old AP # & Title:**

Revision Date: 11/15/2019

EXISTING POLICY / PROCEDURE	OCCA POLICY / PROCEDURE	PROPOSED POLICY / PROCEDURE
~~To prevent identity theft, the Board of Education of Umpqua Community College directs the College to comply with the Federal Trade Commission "Red Flag Rule" which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003 by maintaining and monitoring this program.~~	**References:** 15 U.S. Code Section 1681m(e), (Fair and Accurate Credit Transactions Act) ORS 646A.600 to 646A.628 (Oregon Consumer Identity Theft Protection Act) **NOTE:** *This policy is **legally required**.* ~~The **[*entity*]** is required to provide for the identification, detection, and response to patterns, practices, or specific activities ("Red Flags") that could indicate identity theft of students~~	The College is required to provide for the identification, detection, and response to patterns, practices, or specific activities ("Red Flags") that could indicate identity theft of students when the College serves as a creditor in relation to its students. When applicable, the Chief Financial Officer is directed to develop procedures to implement an Identity Theft Prevention Program (ITPP) to control reasonably foreseeable risks to students from identity theft. **References:** 15 U.S. Code Section 1681m(e), (Fair and Accurate Credit Transactions Act) ORS 646A.600 to 646A.628 (Oregon Consumer Identity Theft Protection Act)

	~~when the **[*entity*]** serves as a creditor in relation to its students. When applicable, the **[*CEO*]** is directed to develop procedures to implement an Identity Theft Prevention Program (ITPP) to control reasonably foreseeable risks to students from identity theft.~~	**RESPONSIBILITY:** The CFO is responsible for implementing and updating this policy. Specific guidance for policy implementation may be found in the associated Administrative Procedure(s).

UMPQUA COMMUNITY COLLEGE

ADMINISTRATIVE PROCEDURE

TITLE: PREVENTION OF IDENTITY THEFT IN STUDENT FINANCIAL TRANSCATIONS

ADMINISTRATIVE PROCEDURE # 5800 ***(was 600.08 Red Flag Rules)***

RELATED TO POLICY # 5800 PREVENTION OF IDENTITY THEFT

I. The Purpose of the Identity Theft Prevention Program

The purpose of this Identity Theft Prevention Program (ITPP) is to control reasonably foreseeable risks to students from identity theft, by providing for the identification, detection, and response to patterns, practices, or specific activities (“Red Flags”) that could indicate identity theft.

II. Definitions

“Identity theft” is a fraud attempted or committed using identifying information of another person without authority.

A. A “creditor” includes government entities who defer payment for goods (for example, payment plans for tuition payments or parking tickets), issued loans or issued student debit cards. Government entities that defer payment for services provided are not considered creditors for purposes of this ITPP.

B. “Deferring payments” refers to postponing payments to a future date and/or installment payments on fines or costs.

C. A “Covered Account” includes one that involves multiple payments or transactions.

D. “Program Administrator” is the individual designated with primary responsibility for oversight of the program.

E. “Person” means any individual who is receiving goods, receives a loan, and/or is issued a debit card from the College and is making payments on a deferred basis for said goods, loan, and/or debit card.

F. “Identifying information” is “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including: name, address, telephone number, social security number, date of birth, government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number, student identification number, computer’s Internet Protocol address, or routing code.

G. Detection or discovery of a “Red Flag” implicates the need to take action under this ITPP to help prevent, detect, and correct identity theft.

III. Detecting “Red Flags” For Potential Identity Theft

A. Risk Factors for Identifying “Red Flags”

The College will consider the following factors in identifying relevant “Red Flags:”

1. the types of covered accounts the College offers or maintains;
2. the methods the College provides to open the College’s covered accounts;
3. the methods the College provides to access the College’s covered accounts; and
4. the College’s previous experience(s) with identity theft.

B. Sources of “Red Flags”

The College will continue to incorporate relevant “Red Flags” into this ITPP from the following sources:

1. incidents of identity theft that the College has experienced;
2. methods of identity theft that the College identifies that reflects changes in identity theft risks; and
3. guidance from the College’s staff who identify changes in identity theft risks.

C. Categories of “Red Flags”

The following Red Flags have been identified for the College’s covered accounts:

1. **Alerts, Notifications, or Warnings from a Consumer Reporting Agency:**
   a. A fraud or active duty alert is included with a consumer report the College receives as part of a background check.

   b. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.

   c. A consumer reporting agency provides a notice of address discrepancy. An address discrepancy occurs when an address provided by a student or an employee substantially differs from the one the credit reporting agency has on file. See Section (V)(10) for specific steps that must be taken to address this situation.

   d. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant, such as:

1) A recent and significant increase in the volume of inquiries;

2) An unusual number of recently established credit relationships;

3) A material change in the use of credit, especially with respect to recently established credit relationships; or

4) An account that was closed for cause or identified for abuse of account privileges by a creditor or financial institution.

2. **Suspicious Documents:**

a. Documents provided for identification appear to have been forged or altered.

b. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

c. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.

d. Other information on the identification is not consistent with readily accessible information that is on file with the College, such as a signature card or a recent check.

e. An application appears to have been altered or forged, or gives the appearance of having been destroyed or reassembled.

I. **Suspicious Personally Identifying Information:**

a. Personal identifying information provided is inconsistent when compared against external information sources used by the College.

For example:

1) The address does not match any address in the consumer report; or

2) The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration’s Death Master File.

b. Personal identifying information provided by a person is not consistent with other personal identifying information provided by the person. For example, there is a lack of correlation between the SSN range and date of birth.

c. Personal identifying information is associated with known fraudulent activity as indicated by internal or third-party sources use by the College. For example:

1) The address on an application is the same as the address provided on a fraudulent application;

2) The phone number on an application is the same as the phone number provided on a fraudulent application;

d. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the College. For example:

1) The address on an application is fictitious, a mail drop, or a prison; or

2) The phone number is invalid, or is associated with a pager or answering service.

e. The SSN provided is the same as that submitted by other persons currently being served by the College.

1) The address or telephone number provided is the same or similar to the account number or telephone number submitted by an unusually large number of other persons being served by the College.

2) The person opening the covered account fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

3) Personal identifying information provided is not consistent with personal identifying information that is on file with the College.

4) The person opening the covered account cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

II. Unusual Use Of – Or Suspicious Activity Relating To – A Covered Account:

a. A new covered account is used in a manner that is commonly associated with known patterns of fraud patterns. For example, a person makes a first payment, but there are no subsequent payments made.

b. A covered account is used in a manner that is not consistent with established patterns of activity on the account. For example, there is:

1) Nonpayment when there is no history of late or missed payments; or

2) A material change in electronic fund transfer patterns in connection with a payment.

c. A covered account that has been inactive for a reasonably lengthy period of time is suddenly used or active.

d. Mail sent to the person holding the covered account is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the person's covered account.

e. The College is notified that the person is not receiving paper account statements.

f. The College is notified of unauthorized transactions in connection with a person's covered account.

Notices From Customers/Persons, Victims of Identity Theft, Law Enforcement Authorities, or Other Businesses About Possible Identity Theft in Connection with Covered Accounts:

The College is notified by a person with a covered account, a victim of identity theft, a law enforcement authority, or any other person, that it has opened a fraudulent account for a person engaged in identity theft.

IV. Measures to Detect "Red Flags"

The College shall do the following to aid in the detection of "Red Flags:"

A. When a new covered account is open, the College shall obtain identifying information about, and information verifying the identity of, the student or other person seeking to open a covered account. Two forms of identification shall be obtained (at least one of which must be a photo identification).

The following are examples of the types of valid identification that a person may provide to verify the identity of the person seeking to open the covered account: valid state-issued driver's license, valid state-issued identification card, current passport, a Social Security Card, current residential lease, or copy of a deed to the person's home or invoice/statement for property taxes.

B. Persons with covered accounts who request a change in their personal information on file, such as a change of address, will have the requested changes verified by the College.

The person shall provide at least one written form of verification reflecting the requested changes to the personal information. For example, if an address change is requested, then documentation evidencing the new address shall be obtained. If a phone number change is requested, then documentation evidencing the new phone number, such as a phone bill, shall be obtained.

V. Preventing and Mitigating Identity Theft

One or more of the following measures, as deemed appropriate under the particular circumstances, shall be implemented to respond to "Red Flags" that are detected:

A. Monitor the covered account for evidence of identity theft;

B. Contact the person who holds the covered account;

C. Change any passwords, security codes, or other security devices that permit access to a covered account;

D. Reopen the covered account with a new account number;

E. Not open a new covered account for the person;

F. Close an existing covered account;

G. Notify the Program Administrator for determination of the appropriate step(s) to take;

H. Not attempt to collect on a covered account or not sell a covered account to a debt collector;

I. Notifying law enforcement;

J. Where a consumer reporting agency provides an address for a consumer that substantially differs from the address that the consumer provided, the College shall take the necessary steps to for a reasonable belief that the College knows the identity of the person for whom the College obtained a credit report, and reconcile the address of the consumer with the credit reporting agency, if the College establishes a continuing relationship with the consumer, and regularly, and in the course of business, provides information to the credit reporting agency; or

K. Determine that no response is warranted under the particular circumstances.

VI. Protect Identifying Information

In order to further prevent the likelihood of Identity Theft occurring with respect to Covered Accounts, the College will take the following steps with respect to its internal operating procedures to protect identifying information:

A. Ensure that its website is secure or provide clear notice that the website is not secure;

B. Ensure complete and secure destruction of paper documents and computer files containing account information when a decision has been made to no longer maintain such information;

C. Ensure that office computers with access to Covered Account information are password protected;

D. Avoid use of social security numbers;

E. Ensure computer virus protection is up to date; and

F. Require and keep only the kinds of information that are necessary for College purposes.

VII. Updating the ITPP

The College shall update this ITPP on an annual basis to reflect changes in risks to persons with covered accounts, or to reflect changes in risks to the safety and soundness of the College from identity theft, based on the following factors:

A. The experiences of the College with identity theft;

B. Changes in methods of identity theft;

1. Changes in methods to detect, prevent and mitigate identity theft;
2. Changes in the types of covered accounts that the College maintains;
3. Changes in the business arrangements of the College, including service provider arrangements.

VIII. Methods for Administering the ITPP

Oversight of the ITPP

Responsibility for developing, implementing and updating this Program lies with an Identity Theft Committee ("Committee") for the College headed by a Program Administrator who may be CFO or his or her appointee. The remainder of the committee membership comprises administrative positions from the areas of Human Resources, Information Technology, and Student Services. The Program Administrator will be responsible for ensuring appropriate training of College staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Program.

Oversight by the Program Administrator shall include:

A. Assigning specific responsibility for the ITPP's implementation;

B. Reviewing reports prepared by the staff regarding compliance of the ITPP; and

C. Approving material changes to the ITPP as necessary to address changing identity theft risks.

IX. Reports

A. In General – Staff responsible for the development, implementation, and administration of this ITPP shall report to the Program Administrator on an annual basis.

B. Contents of Report – The report shall address material matters to the ITPP and evaluate the following issues: the effectiveness of the policies and procedures in addressing the risk of identity theft in connection with opening new covered accounts and with respect to existing covered accounts; service provider arrangements; significant incidents involving identity theft and management's response; and recommendations for material changes to the ITPP.

C. **Oversight of Service Provider Arrangements** – Whenever the College engages a service provider to perform an activity in connection with one or more covered accounts the College shall take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. To that end, the College shall require our service contractors, by contract, to have policies and procedures to detect relevant "Red Flags" that may arise in the performance of the service provider's activities, and either report the "Red Flags" to the College, or to take appropriate steps to prevent or mitigate identity theft.

References:
15 U.S. Code Section 1681m(e) (Fair and Accurate Credit Transactions Act (FACT ACT or FACTA))

ORS 646A.604(8) (notice exception – Oregon Consumer Identity Theft Protection Act)

RESPONSIBILITY:
The CFO is responsible for implementing and updating this procedure.

NEXT REVIEW DATE:
DATE OF ADOPTION:
DATE(S) OF REVISION:
DATE(S) OF PRIOR REVIEW:

POLICY / ADMINISTRATIVE PROCEDURE CONVERSION TEMPLATE

Complete for Conversions Only

TITLE: Prevention of Identity Theft in Student Financial Transactions

New BP #: **Old BP # & Title:**

New AP #: 5800 **Old AP # & Title:** 600.08 Red Flag Rules

Revision Date: 11/15/2019

EXISTING POLICY / PROCEDURE	OCCA POLICY / PROCEDURE	PROPOSED POLICY / PROCEDURE
II. DEFINITIONS AND PROGRAM A. Red Flags Rule Definitions Used in this Program ~~“Identity Theft” is a “fraud committed or attempted using the identifying information of another person without authority.”~~ ~~A “Red Flag” is a “pattern, practice, or specific activity that indicates the possible existence of Identity Theft.”~~ ~~A “Covered Account” includes all accounts that permit multiple transactions or poses a reasonable foreseeable risk of being used to promote identity theft.~~ ~~“Program Administrator” is the individual designated with primary responsibility for oversight of the program.~~ See Section VI below.	**Reference:** 15 U.S. Code Section 1681m(e) (Fair and Accurate Credit Transactions Act (FACT ACT or FACTA)) ORS 646A.604(8) (notice exception – Oregon Consumer Identity Theft Protection Act) **NOTE:** *This procedure is **legally required**.* **I. The Purpose of the Identity Theft Prevention Program** ~~The purpose of this Identity Theft Prevention Program (ITPP) is to control reasonably foreseeable risks to students from identity theft, by providing for the identification, detection, and response to patterns,~~	**I. The Purpose of the Identity Theft Prevention Program** The purpose of this Identity Theft Prevention Program (ITPP) is to control reasonably foreseeable risks to students from identity theft, by providing for the identification, detection, and response to patterns, practices, or specific activities (“Red Flags”) that could indicate identity theft. **II. Definitions** “Identity theft” is a fraud attempted or committed using identifying information of another person without authority. A “creditor” includes government entities who defer payment for goods

~~“Identifying information” is “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including: name, address, telephone number, social security number, date of birth, government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number, student identification number, computer’s Internet Protocol address, or routing code.~~ B. Fulfilling Requirements of the Red Flags Rule Under the Red Flags Rule, the College is required to establish an “Identity Theft Prevention Program” tailored to its size, complexity and the nature of its operation. Each program must contain reasonable policies and procedures to: 1. Identify relevant Red Flags for new and existing covered accounts and incorporate those Red Flags into the Program; 2. Detect Red Flags that have been incorporated into the Program; 3. Respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft; and 4. Ensure the Program is updated periodically to reflect changes in risks	~~practices, or specific activities (“Red Flags”) that could indicate identity theft.~~ **II. Definitions** “~~Identity theft” is a fraud attempted or committed using identifying information of another person without authority~~. A “creditor” includes government entities who defer payment for goods (for example, payment plans for bookstore accounts or parking tickets), issued loans or issued student debit cards. Government entities that defer payment for services provided are not considered creditors for purposes of this ITPP. “Deferring payments” refers to postponing payments to a future date and/or installment payments on fines or costs. ~~A “covered account” includes one that involves multiple payments or transactions.~~ “Person” means any individual who is receiving goods, receives a loan, and/or is issued a debit card from the **[*entity*]** and is making payments on a deferred basis for said goods, loan, and/or debit card. ~~Detection or discovery of a “Red Flag” implicates the need to take action~~	(for example, payment plans for tuition payments or parking tickets), issued loans or issued student debit cards. Government entities that defer payment for services provided are not considered creditors for purposes of this ITPP. “Deferring payments” refers to postponing payments to a future date and/or installment payments on fines or costs. A “Covered Account” includes one that involves multiple payments or transactions. “Program Administrator” is the individual designated with primary responsibility for oversight of the program. “Person” means any individual who is receiving goods, receives a loan, and/or is issued a debit card from the College and is making payments on a deferred basis for said goods, loan, and/or debit card. “Identifying information” is “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including: name, address, telephone number, social security number, date of birth, government issued driver’s license or identification number, alien registration number, government passport number, employer or

to students, employees or other persons, or their safety and soundness from Identity Theft. III. IDENTIFICATION OF RED FLAGS ~~In order to identify relevant Red Flags, the College considers the types of accounts that it offers and maintains, methods it provides to open its accounts, methods it provides to access its accounts, and its previous experiences with Identity Theft~~. The College identifies the following Red Flags in each of the listed categories: A. ~~Notifications and Warnings from Credit Reporting Agencies~~ ~~Red Flags~~ ~~1. Report of fraud accompanying a credit report;~~ ~~2. Notice or report from a credit agency of a credit freeze on an applicant;~~ ~~3. Notice or report from a credit agency of an active duty alert for an applicant;~~ ~~4. Receipt of a notice of address discrepancy in response to a credit report request; and~~ ~~5. Indication from a credit report of activity that is inconsistent with an applicant's usual pattern or activity.~~ B~~. Suspicious Documents~~	~~under this ITPP to help prevent, detect, and correct identity theft.~~ **III. Detecting “Red Flags” For Potential Identity Theft** ~~**A. Risk Factors for Identifying “Red Flags”**~~ ~~The **[*entity*]** will consider the following factors in identifying relevant “Red Flags:”~~ ~~1) the types of covered accounts the **[*entity*]** offers or maintains;~~ ~~2) the methods the **[*entity*]** provides to open the **[*entity’s*]** covered accounts;~~ ~~3) the methods the **[*entity*]** provides to access the **[*entity’s*]** covered accounts; and~~ ~~4) the ***[entity]***’s previous experience(s) with identity theft.~~ **B. Sources of “Red Flags”** ~~The **[*entity*]** will continue to incorporate relevant “Red Flags” into this ITPP from the following sources:~~ ~~1) incidents of identity theft that the **[*entity*]** has experienced;~~ ~~2) methods of identity theft that the **[*entity*]** identifies that reflects changes in identity theft risks; and~~	taxpayer identification number, student identification number, computer’s Internet Protocol address, or routing code. Detection or discovery of a “Red Flag” implicates the need to take action under this ITPP to help prevent, detect, and correct identity theft. **III. Detecting “Red Flags” For Potential Identity Theft** **A. Risk Factors for Identifying “Red Flags”** The College will consider the following factors in identifying relevant “Red Flags:” 1) the types of covered accounts the College offers or maintains; 2) the methods the College provides to open the College’s covered accounts; 3) the methods the College provides to access the College’s covered accounts; and 4) the College’s previous experience(s) with identity theft. **B. Sources of “Red Flags”** The College will continue to incorporate relevant “Red Flags” into this ITPP from the following sources:

~~Red Flags~~ ~~1. Identification document or card that appears to be forged, altered or inauthentic;~~ ~~2. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;~~ ~~3. Other document with information that is not consistent with existing information; and~~ ~~4. Application for service that appears to have been altered or forged.~~ C. ~~Suspicious Personal Identifying Information~~ ~~Red Flags~~ ~~1. Identifying information presented that is inconsistent with other information the person provides (example: inconsistent birth dates);~~ ~~2. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a loan application);~~ ~~3. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;~~	~~3) guidance from the **[*entity's*]** supervisor's who identify changes in identity theft risks.~~ **C. Categories of "Red Flags"** The following Red Flags have been identified for the **[*entity*]**'s covered accounts: ~~**Alerts, Notifications, or Warnings from a Consumer Reporting Agency:**~~ ~~1) A fraud or active duty alert is included with a consumer report the **[*entity*]** receives as part of a background check.~~ ~~2) A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.~~ ~~3) A consumer reporting agency provides a notice of address discrepancy. An address discrepancy occurs when an address provided by a student substantially differs from the one the credit reporting agency has on file. See Section (V)(9) for specific steps that must be taken to address this situation.~~	1) incidents of identity theft that the College has experienced; 2) methods of identity theft that the College identifies that reflects changes in identity theft risks; and 3) guidance from the College's staff who identify changes in identity theft risks. **C. Categories of "Red Flags"** The following Red Flags have been identified for the College's covered accounts: **Alerts, Notifications, or Warnings from a Consumer Reporting Agency:** 1) A fraud or active duty alert is included with a consumer report the College receives as part of a background check. 2) A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report. 3) A consumer reporting agency provides a notice of address discrepancy. An address discrepancy occurs when an address provided by a student or an employee substantially differs from the one the credit reporting agency has on file. See Section (V)(10) for specific

~~4. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);~~ ~~5. Social security number presented that is the same as one given by another person;~~ ~~6. An address or phone number presented that is the same as that of another person;~~ ~~7. A person fails to provide complete personal identifying information on an application when reminded to do so; and~~ ~~8. A person's identifying information is not consistent with the information that is on file.~~ D. ~~Suspicious Covered Account Activity or Unusual Use of Account Red Flags~~ ~~1. Change of address for an account followed by a request to change the account holder's name;~~ ~~2. Payments stop on an otherwise consistently up-to-date account;~~ ~~3. Account used in a way that is not consistent with prior use;~~ ~~4. Mail sent by the College is repeatedly returned as undeliverable;~~	~~4) A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant, such as:~~ ~~(a) A recent and significant increase in the volume of inquiries;~~ ~~(b) An unusual number of recently established credit relationships;~~ ~~(c) A material change in the use of credit, especially with respect to recently established credit relationships; or~~ ~~(d) An account that was closed for cause or identified for abuse of account privileges by a creditor or financial institution.~~ ~~**Suspicious Documents:**~~ ~~1) Documents provided for identification appear to have been forged or altered.~~ ~~2) The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.~~	steps that must be taken to address this situation. 4) A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant, such as: (a) A recent and significant increase in the volume of inquiries; (b) An unusual number of recently established credit relationships; (c) A material change in the use of credit, especially with respect to recently established credit relationships; or (d) An account that was closed for cause or identified for abuse of account privileges by a creditor or financial institution. **Suspicious Documents:** 1) Documents provided for identification appear to have been forged or altered. 2) The photograph or physical description on the identification is not consistent with the appearance of the applicant or

~~5. Notice to the College that a person is not receiving mail sent by the College;~~ ~~6. Notice to the College that an account has unauthorized activity;~~ ~~7. Breach in the College's computer system security; and~~ ~~8. Unauthorized access to or use of account information.~~ ~~E. Alerts from Others~~ ~~Red Flag~~ ~~1. Notice to the College from a student, Identity Theft victim, law enforcement or other person that the College has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.~~ IV. DETECTING RED FLAGS A. Student Enrollment / New Employee and Other Persons Accounts ~~In order to detect any of the Red Flags identified above associated with the enrollment of a student, new employees or other persons, College personnel will take the following steps to obtain and verify the identity of the person opening the account:~~ ~~Detect~~ ~~1. Require certain identifying information such as name, date of~~	~~3) Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.~~ ~~4) Other information on the identification is not consistent with readily accessible information that is on file with the **[*entity*]**, such as a signature card or a recent check.~~ ~~5) An application appears to have been altered or forged, or gives the appearance of having been destroyed or reassembled.~~ ~~**Suspicious Personally Identifying Information:**~~ ~~1) Personal identifying information provided is inconsistent when compared against external information sources used by the **[*entity*]**.~~ ~~For example:~~ ~~(a) The address does not match any address in the consumer report; or~~ ~~(b) The Social Security Number (SSN) has~~	customer presenting the identification. 3) Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification. 4) Other information on the identification is not consistent with readily accessible information that is on file with the College, such as a signature card or a recent check. 5) An application appears to have been altered or forged, or gives the appearance of having been destroyed or reassembled. **Suspicious Personally Identifying Information:** 1) Personal identifying information provided is inconsistent when compared against external information sources used by the College. For example: (a) The address does not match any address in the consumer report; or

~~birth, academic records, home address or other identification; and~~ ~~2. Verify the student's identity at time of issuance of student identification card (review of driver's license or other government-issued photo identification).~~ B. Existing Accounts ~~In order to detect any of the Red Flags identified above for an existing Covered Account, UCC personnel will take the following steps to monitor transactions on an account:~~ ~~Detect~~ ~~1. Verify the identification of persons if they request information (in person, via telephone, via facsimile, via email);~~ ~~2. Verify the validity of requests to change billing addresses by mail or email and provide reasonable means of promptly reporting incorrect billing address changes; and~~ 3. Verify changes in banking information given for billing and payment purposes. C~~. Consumer ("Credit") Report Requests~~ ~~In order to detect any of the Red Flags identified above for an employment or volunteer position for which a credit or background report is sought, College personnel will take the following steps~~	~~not been issued, or is listed on the Social Security Administration's Death Master File.~~ ~~2) Personal identifying information provided by a person is not consistent with other personal identifying information provided by the person. For example, there is a lack of correlation between the SSN range and date of birth.~~ ~~3) Personal identifying information is associated with known fraudulent activity as indicated by internal or third-party sources use by the **[*entity*]**. For example:~~ ~~(a) The address on an application is the same as the address provided on a fraudulent application;~~ ~~(b) The phone number on an application is the same as the phone number provided on a fraudulent application;~~ ~~4) Personal identifying information provided is of a type commonly associated with~~	(b) The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File. 2) Personal identifying information provided by a person is not consistent with other personal identifying information provided by the person. For example, there is a lack of correlation between the SSN range and date of birth. 3) Personal identifying information is associated with known fraudulent activity as indicated by internal or third-party sources use by the College. For example: (a) The address on an application is the same as the address provided on a fraudulent application; (b) The phone number on an application is the same as the phone number provided on a fraudulent application;

~~to assist in identifying address discrepancies:~~ ~~1. Require written verification from any applicant that the address provided by the applicant is accurate at the time the request for the background check or credit report is made to the consumer reporting agency; and~~ 2. In the event that notice of an address discrepancy is received, verify that the background check or credit report pertains to the applicant for whom the requested report was made and report to the consumer reporting agency an address for the applicant that the College has reasonably confirmed is accurate. V. PREVENTING AND MITIGATING IDENTITY THEFT In the event Umpqua Community College personnel detect any identified Red Flags, such personnel shall take one or more of the following steps, depending on the degree of risk posed by the Red Flag: Prevent and Mitigate 1~~. Continue to monitor a Covered Account for evidence of Identity Theft;~~ 2. ~~Contact the student or applicant~~ (for which a background check or credit report was run);	~~fraudulent activity as indicated by internal or third-party sources used by the **[*entity*]**. For example:~~ ~~(a) The address on an application is fictitious, a mail drop, or a prison; or~~ ~~(b) The phone number is invalid, or is associated with a pager or answering service.~~ ~~5) The SSN provided is the same as that submitted by other persons currently being served by the **[*entity*]**.~~ ~~6) The address or telephone number provided is the same or similar to the account number or telephone number submitted by an unusually large number of other persons being served by the **[*entity*]**.~~ ~~7) The person opening the covered account fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.~~ ~~8) Personal identifying information provided is not~~	4) Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the College. For example: (a) The address on an application is fictitious, a mail drop, or a prison; or (b) The phone number is invalid, or is associated with a pager or answering service. 5) The SSN provided is the same as that submitted by other persons currently being served by the College. 6) The address or telephone number provided is the same or similar to the account number or telephone number submitted by an unusually large number of other persons being served by the College. 7) The person opening the covered account fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

3. ~~Change any passwords or other security devices that permit access to Covered Accounts;~~ 4. ~~Not open a new Covered Account;~~ 5. ~~Provide the person with a new identification number;~~ 6. Notify the Program Administrator for determination of the appropriate step(s) to take; 7~~. Notify law enforcement;~~ 8. File or assist in filing a Suspicious Activities Report ("SAR"); or 9. ~~Determine that no response is warranted under the particular circumstances.~~ **Protect Identifying Information** In order to further prevent the likelihood of Identity Theft occurring with respect to Covered Accounts, the College will take the following steps with respect to its internal operating procedures to protect identifying information: 1. Ensure that its website is secure or provide clear notice that the website is not secure; 2. Ensure complete and secure destruction of paper documents and computer files containing account information when a decision has been	~~consistent with personal identifying information that is on file with the **[*entity*]**.~~ ~~9) The person opening the covered account cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.~~ **Unusual Use Of – Or Suspicious Activity Relating To – A Covered Account:** 1) A new covered account is used in a manner that is commonly associated with known patterns of fraud patterns. For example, a person makes a first payment, but there are no subsequent payments made. 2) A covered account is used in a manner that is not consistent with established patterns of activity on the account. For example, there is: (a) Nonpayment when there is no history of late or missed payments; or (b) A material change in electronic fund transfer patterns in	8) Personal identifying information provided is not consistent with personal identifying information that is on file with the College. 9) The person opening the covered account cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report. **Unusual Use Of – Or Suspicious Activity Relating To – A Covered Account:** 1) A new covered account is used in a manner that is commonly associated with known patterns of fraud patterns. For example, a person makes a first payment, but there are no subsequent payments made. 2) A covered account is used in a manner that is not consistent with established patterns of activity on the account. For example, there is: (a) Nonpayment when there is no history of late or missed payments; or (b) A material change in electronic fund transfer patterns in

made to no longer maintain such information; 3. Ensure that office computers with access to Covered Account information are password protected; 4. Avoid use of social security numbers; 5. Ensure computer virus protection is up to date; and 6. Require and keep only the kinds of information that are necessary for College purposes. VI. PROGRAM ADMINISTRATION A. Oversight Responsibility for developing, implementing and updating this Program lies with an Identity Theft Committee ("Committee") for the College. The Committee is headed by a Program Administrator who may be the President of the College or his or her appointee. Two or more other individuals appointed by the President of the College or the Program Administrator comprise the remainder of the committee membership. The Program Administrator will be responsible for ensuring appropriate training of College staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and	connection with a payment. 3) A covered account that has been inactive for a reasonably lengthy period of time is suddenly used or active. 4) Mail sent to the person holding the covered account is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the person's covered account. 5) The **[*entity*]** is notified that the person is not receiving paper account statements. 6) The **[*entity*]** is notified of unauthorized transactions in connection with a person's covered account. ~~**Notices From Customers/Persons, Victims of Identity Theft, Law Enforcement Authorities, or Other Businesses About Possible Identity Theft in Connection with Covered Accounts:**~~ ~~The **[*entity*]** is notified by a person with a covered account, a victim of identity theft, a law enforcement~~	connection with a payment. 3) A covered account that has been inactive for a reasonably lengthy period of time is suddenly used or active. 4) Mail sent to the person holding the covered account is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the person's covered account. 5) The College is notified that the person is not receiving paper account statements. 6) The College is notified of unauthorized transactions in connection with a person's covered account. **Notices From Customers/Persons, Victims of Identity Theft, Law Enforcement Authorities, or Other Businesses About Possible Identity Theft in Connection with Covered Accounts:** The College is notified by a person with a covered account, a victim of identity theft, a law enforcement

mitigating Identity Theft, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Program. B. Staff Training and Reports College staff responsible for implementing the Program shall be trained either by or under the direction of the Program Administrator in the detection of Red Flags and the responsive steps to be taken when a Red Flag is detected. College staff shall be trained, as necessary, to effectively implement the Program. College employees are expected to notify the Program Administrator once they become aware of an incident of Identity Theft or of the College's failure to comply with this Program. At least annually or as otherwise requested by the Program Administrator, College staff responsible for development, implementation, and administration of the Program shall report to the Program Administrator on compliance with this Program. The report should address such issues as effectiveness of the policies and procedures in addressing the risk of identity theft in connection with the opening and maintenance of Covered Accounts, service provider arrangements, significant incidents involving identity theft and management's response,	~~authority, or any other person, that it has opened a fraudulent account for a person engaged in identity theft.~~ **IV. Measures to Detect "Red Flags**" ~~The **[*entity*]** shall do the following to aid in the detection of "Red Flags:"~~ ~~1)~~ ~~When a new covered account is open, the **[*entity*]** shall obtain identifying information about, and information verifying the identity of, the student or other person seeking to open a covered account. Two forms of identification shall be obtained (at least one of which must be a photo identification).~~ ~~The following are examples of the types of valid identification that a person may provide to verify the identity of the person seeking to open the covered account: valid state-issued driver's license, valid state-issued identification card, current passport, a Social Security Card, current residential lease, or copy of a deed to the person's home or~~	authority, or any other person, that it has opened a fraudulent account for a person engaged in identity theft. **IV. Measures to Detect "Red Flags**" The College shall do the following to aid in the detection of "Red Flags:" 1) When a new covered account is open, the College shall obtain identifying information about, and information verifying the identity of, the student or other person seeking to open a covered account. Two forms of identification shall be obtained (at least one of which must be a photo identification). The following are examples of the types of valid identification that a person may provide to verify the identity of the person seeking to open the covered account: valid state-issued driver's license, valid state-issued identification card, current passport, a Social Security Card, current residential lease, or copy of a deed to the person's home or

and recommendations for changes to the Program. C. Service Provider Arrangements In the event the College engages a service provider to perform an activity in connection with one or more Covered Accounts, the College will take the following steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of Identity Theft. 1. Require, by contract, that service providers have such policies and procedures in place; and 2. Require, by contract, that service providers review the College's Program and report any Red Flags to the Program Administrator or the College employee with primary oversight of the service provider relationship. D. Non-disclosure of Specific Practices For the effectiveness of this Identity Theft Prevention Program, knowledge about specific Red Flag identification, detection, mitigation and prevention practices may need to be limited to the Committee who developed this Program and to those employees with a need to know them. Any documents that may have been produced or are produced in order to develop or implement this program that list or	~~invoice/statement for property taxes.~~ ~~2) Persons with covered accounts who request a change in their personal information on file, such as a change of address, will have the requested changes verified by the **[*entity*]**.~~ ~~The person shall provide at least one written form of verification reflecting the requested changes to the personal information. For example, if an address change is requested, then documentation evidencing the new address shall be obtained. If a phone number change is requested, then documentation evidencing the new phone number, such as a phone bill, shall be obtained.~~ **V. Preventing and Mitigating Identity Theft** One or more of the following measures, as deemed appropriate under the particular circumstances, shall be implemented to respond to “Red Flags” that are detected: 1) ~~Monitor the covered account for evidence of identity theft~~;	invoice/statement for property taxes. 2) Persons with covered accounts who request a change in their personal information on file, such as a change of address, will have the requested changes verified by the College. The person shall provide at least one written form of verification reflecting the requested changes to the personal information. For example, if an address change is requested, then documentation evidencing the new address shall be obtained. If a phone number change is requested, then documentation evidencing the new phone number, such as a phone bill, shall be obtained. **V. Preventing and Mitigating Identity Theft** One or more of the following measures, as deemed appropriate under the particular circumstances, shall be implemented to respond to “Red Flags” that are detected:

describe such specific practices and the information those documents contain are considered “confidential” and should not be shared with other employees or the public. The Program Administrator shall inform the Committee and those employees with a need to know the information of those documents or specific practices which should be maintained in a confidential manner. E. Program Updates The Committee will periodically review and update this Program to reflect changes in risks to students, employees / other persons and the soundness of the College from Identity Theft. In doing so, the Committee will consider the College's experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, and changes in the College's business arrangements with other entities. After considering these factors, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Committee will update the Program.	2) ~~Contact the person who holds the covered account~~; ~~3) Change any passwords, security codes, or other security devices that permit access to a covered account;~~ ~~4) Reopen the covered account with a new account number;~~ ~~5) Not open a new covered account for the person;~~ 6) Close an existing covered account; 7) Not attempt to collect on a covered account or not sell a covered account to a debt collector; ~~8) Notifying law enforcement;~~ 9) Where a consumer reporting agency provides an address for a consumer that substantially differs from the address that the consumer provided, the **[*entity*]** shall take the necessary steps to for a reasonable belief that the **[*entity*]** knows the identity of the person for whom the **[*entity*]** obtained a credit report, and reconcile the address of the consumer with the credit reporting agency, if the **[*entity*]** establishes a continuing relationship with the consumer, and regularly, and in the course of	1) Monitor the covered account for evidence of identity theft; 2) Contact the person who holds the covered account; 3) Change any passwords, security codes, or other security devices that permit access to a covered account; 4) Reopen the covered account with a new account number; 5) Not open a new covered account for the person; 6) Close an existing covered account; 7) Notify the Program Administrator for determination of the appropriate step(s) to take; 8) Not attempt to collect on a covered account or not sell a covered account to a debt collector; 9) Notifying law enforcement; 10) Where a consumer reporting agency provides an address for a consumer that substantially differs from the address that the consumer provided, the College shall take the necessary steps to for a reasonable belief that the College knows the identity of the person for whom the College obtained a credit

	business, provides information to the credit reporting agency; or 10) Determine that no response is warranted under the particular circumstances. **VI. Updating the ITPP** The **[*entity*]** shall update this ITPP on an annual basis to reflect changes in risks to persons with covered accounts, or to reflect changes in risks to the safety and soundness of the **[*entity*]** from identity theft, based on the following factors: 1) The experiences of the **[*entity*]** with identity theft; 2) Changes in methods of identity theft; 3) Changes in methods to detect, prevent and mitigate identity theft; 4) Changes in the types of covered accounts that the **[*entity*]** maintains; 5) Changes in the business arrangements of the **[*entity*]**, including service provider arrangements. **VII. Methods for Administering the ITPP** **A. Oversight of the ITPP** Oversight by the ’s **[*designate position*]** shall include:	report, and reconcile the address of the consumer with the credit reporting agency, if the College establishes a continuing relationship with the consumer, and regularly, and in the course of business, provides information to the credit reporting agency; or 11) Determine that no response is warranted under the particular circumstances. **VI. Protect Identifying Information** In order to further prevent the likelihood of Identity Theft occurring with respect to Covered Accounts, the College will take the following steps with respect to its internal operating procedures to protect identifying information: 1. Ensure that its website is secure or provide clear notice that the website is not secure; 2. Ensure complete and secure destruction of paper documents and computer files containing account information when a decision has been made to no longer maintain such information; 3. Ensure that office computers with access to Covered Account information are password protected;

	1) Assigning specific responsibility for the ITPP's implementation; 2) Reviewing reports prepared by the staff regarding compliance of the ITPP; and 3) Approving material changes to the ITPP as necessary to address changing identity theft risks. **B. Reports** 1) **In General** – Staff responsible for the development, implementation, and administration of this ITPP shall report to the Board of Education on an annual basis. 2) **Contents of Report** – The report shall address material matters to the ITPP and evaluate the following issues: the effectiveness of the policies and procedures in addressing the risk of identity theft in connection with opening new covered accounts and with respect to existing covered accounts; service provider arrangements; significant incidents involving identity theft and management's	4. Avoid use of social security numbers; 5. Ensure computer virus protection is up to date; and 6. Require and keep only the kinds of information that are necessary for College purposes. **VII. Updating the ITPP** The College shall update this ITPP on an annual basis to reflect changes in risks to persons with covered accounts, or to reflect changes in risks to the safety and soundness of the College from identity theft, based on the following factors: 1) The experiences of the College with identity theft; 2) Changes in methods of identity theft; 3) Changes in methods to detect, prevent and mitigate identity theft; 4) Changes in the types of covered accounts that the College maintains; 5) Changes in the business arrangements of the College, including service provider arrangements. **VIII. Methods for Administering the ITPP** **Oversight of the ITPP**

	response; and recommendations for material changes to the ITPP. 3) **Oversight of Service Provider Arrangements** – Whenever the **[*entity*]** engages a service provider to perform an activity in connection with one or more covered accounts the **[*entity*]** shall take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. To that end, the **[*entity*]** shall require our service contractors, by contract, to have policies and procedures to detect relevant “Red Flags” that may arise in the performance of the service provider’s activities, and either report the “Red Flags” to the **[*entity*]**, or to take appropriate steps to prevent or mitigate identity theft.	Responsibility for developing, implementing and updating this Program lies with an Identity Theft Committee (“Committee”) [NB1]for the College. The Committee is headed by a Program Administrator who may be the President of the College or his or her appointee. Two or more other individuals appointed by the President of the College or the Program Administrator comprise the remainder of the committee membership. The Program Administrator will be responsible for ensuring appropriate training of College staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Program. Oversight by the Program Administrator shall include: 1) Assigning specific responsibility for the ITPP’s implementation; 2) Reviewing reports prepared by the staff regarding compliance of the ITPP; and 3) Approving material changes to the ITPP as necessary to

		address changing identity theft risks. **D. Reports** **1) In General** – Staff responsible for the development, implementation, and administration of this ITPP shall report to the Program Administrator on an annual basis. **2) Contents of Report** – The report shall address material matters to the ITPP and evaluate the following issues: the effectiveness of the policies and procedures in addressing the risk of identity theft in connection with opening new covered accounts and with respect to existing covered accounts; service provider arrangements; significant incidents involving identity theft and management’s response; and recommendations for material changes to the ITPP. **3) Oversight of Service Provider Arrangements** – Whenever the College engages a service provider to perform an activity in connection with one or more covered accounts the College shall take steps to ensure that

		the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. To that end, the College shall require our service contractors, by contract, to have policies and procedures to detect relevant “Red Flags” that may arise in the performance of the service provider’s activities, and either report the “Red Flags” to the College, or to take appropriate steps to prevent or mitigate identity theft. **Reference:** 15 U.S. Code Section 1681m(e) (Fair and Accurate Credit Transactions Act (FACT ACT or FACTA)) ORS 646A.604(8) (notice exception – Oregon Consumer Identity Theft Protection Act) **RESPONSIBILITY:** The CFO is responsible for implementing and updating this procedure.

BOARD OF EDUCATION UMPQUA COMMUNITY COLLEGE DOUGLAS COUNTY, OREGON	__X__ Information Item ____ Action Item
Subject: Discuss a Bond for Capital Improvements	Date: March 11, 2020
The Board will discuss asking voters to consider a bond in November 2020 to fund capital improvements to Umpqua Community College.	
Recommendation by:	Approved for Consideration: Debra Thatcher