Student Verification Procedure

In compliance with Federal Regulations, Central Christian College is required to verify the identity of students who participate in distance learning or online courses and establish that students who register in these courses are the same students who participate in and complete the course activities and assessments and receive academic credit.

During the application and admission process, student identity is vetted in accordance with standard practices. Students are responsible for providing their complete and true identity information in any identification verification process and it is against policy for students to give account credentials to any other party.

Upon application, each student receives a unique and secure CCCK user account. This user account allows the student to authenticate into CCCK systems, including the Learning Management Systems (LMS) and the student portal. Students have the ability to change their password and are encouraged to do so periodically. The College's Information Technology department is responsible for creating user accounts using a FERPA compliant procedure.

Central Christian College of Kansas uses CANVAS as its learning management system. This system integrates with the College's authentication services to ensure appropriate and secure student access to courses and other Student Information Systems. All users of the learning management system are responsible for maintaining the security of their login credentials. Attempting to discover another user's password or attempts to gain unauthorized access to another person's files or email is prohibited.

All students participating in distance education courses must log in to their course using their CCCK credentials. This secure login is a student's only means of access to the LMS. Students are registered in their courses through the SIS, which transmits registration information directly into the LMS without any action on the part of students, faculty, or staff beyond the regular registration process. Only duly registered students and the instructor of record appear on the roster of any distance education course. Furthermore, every action within a course site registers on the extensive tracking features of the LMS, which track each user in terms of time and duration of the action and part of the site involved, even if there is no posting by the students. In the LMS, the email system, and other applicable systems, students can associate a photo with their account, allowing for visual identification of the student. Technology for live audio and/or visual communication, which can be helpful in verifying student identity, is also available for faculty, staff, and students. Faculty can view official ID photo images of students as part of their class rosters in the SIS, if they so choose.

Any online student work, assessments or activities that are graded or contribute to a student's grade must be submitted via the LMS. Proctored exams are not required of students enrolled at CCCK, as any exams or quizzes are accessed through the College's LMS, which requires a college provided unique username and password. Plagiarism detection tools are available to help determine the identity of those who submit the work. Exams can require a passcode as offered to students by the instructor. The system also allows for moderated test-taking, if in the view of the instructor there is a need to utilize. This is at no extra vost to the student.

Faculty teaching courses through distance education methods hold primary responsibility for ensuring that this method of verification protects student privacy. As technology and personal accountability are

not absolute in determining a student's identity, faculty members are encouraged to remain vigilant if an assignment or post seems non-representative of the student's normal work.

All users of the College's learning management system are responsible for maintaining the security of usernames, passwords, and other access credentials as required. An account is given to an individual for the exclusive use by that individual. Attempting to discover another user's password or attempts to gain unauthorized access to another person's files or mail is prohibited. It is against College policy for a user to give someone his or her password or allow others to use his or her account. Users are responsible for any and all users of their account. Users are responsible for all activity on their accounts.

All official communication is sent through a ".edu" address, which is specific to the student and also requires a password. Student should use this email address for communications with faculty and staff.

The College maintains student biographic, demographic, admission, and enrollment records in the College's SIS. Access to this information requires valid College network credentials, in addition to authorization controls within the LMS and/or SIS.

All students are required to communicate with faculty utilizing their official college email or through the LMS. Course related communication is facilitated through the LMS or student college email. Once a student is enrolled with the college, staff and faculty only communicate utilizing the college issued student email. Faculty and Staff will not respond to student's emails unless the LMS or college email is utilized as the communication tool.

All Zoom sessions require a password. Students entering the zoom session must use their full name and have their camera on the entire session. Students can be maintained in the zoom "waiting room" until the student's authentication can be verified for the zoom meeting. Zoom is embedded into the LMS to provide an additional measure of authentication and privacy. Students are issued a unique Student ID from the SIS.

In some cases, faculty may require student to verify understanding of these policies and to ensure a picture has been uploaded into the student profile, to be used as an aid in student verification.