VERIFICATION OF STUDENT IDENTITY IN ONLINE PROGRAMS

In order to assist students in understanding their legal and ethical responsibilities as online participants in the academic community, and in compliance with the Higher Education Opportunity Act, specifically Public Law 110-35, St. John Fisher University has developed the following policies and procedures.
The Act itself requires that accrediting agencies require postsecondary institutions that "offer distance education or correspondence education…have processes through which the institution establishes that the student who registers in a distance education or correspondence education course or program is the same student who participates in and completes the program and receives the academic credit."

St. John Fisher University's Office of Information Technology (OIT) has already established clear guidelines for appropriate use of computer and information technology resources. The full text of these policies is available at https://sjfc.teamdynamix.com/TDClient/1811/Portal/KB/ArticleDet?ID=34295, but some of the pertinent language is excerpted below.

> **OIT Appropriate Use Policy**
> "The University expects all members of the St. John Fisher community to use computing and information technology resources in a responsible manner and to respect the public trust through which these resources have been provided, the rights and privacy of others, the integrity of facilities and controls, and all pertinent laws and University policies and standards…. The computing and information technology resources at St. John Fisher University are to be used in a responsible, ethical, and legal manner.
> Users of the University's computing and information technology resources are expected to act in accordance with the (University's) policies and with local, state, and federal law identified in but not limited to, the Telecommunication Act of 1995, the Patriot Act, and New York State Article 156."
>
> **Appropriate use** guidelines include (but are not limited to) the following:
> Use only those computing and information technology resources for which you have authorization;
> Protect the access and integrity of computing and information technology resources;
>
> **Policy violations** include, but are not limited to the following:
> Using someone else's account and password or sharing your account and password with someone else;
> Using computing and information technology resources you have not been specifically authorized to use including another user's electronic mail, data, or programs;
> Forging or in any way misrepresenting your identity;
> Purposely looking for or exploiting security flaws to gain system or data access;
>
> **Enforcement** of this University policy may include, among other actions, any or all of the following actions if users violate this policy:
>
> Disciplinary action, up to and including reassignment or removal from University housing and/or suspension or expulsion from the University;
>
> Persons violating this policy may be subject to loss of computing privileges at the University and/or prosecution under applicable civil or criminal laws.

Other relevant policy includes the **SJF Academic Integrity Policy** (available at https://www.sjf.edu/policies/academic-integrity), which defines violations of academic integrity as the

misrepresentation of work ownership/authorship and asserts that “every student is expected to demonstrate academic integrity in all academic pursuits at all times.”

PROCEDURES FOR ST. JOHN FISHER UNIVERSITY ACCOUNT CREATION & MAINTENANCE

Newly accepted students receive an SJF ID and pin, and once deposited the student will receive a network account. SJF IDs are used to access the student information system, Fish’R’Net, to complete a number of tasks, including registering for classes, accepting financial aid and paying their bill. Network accounts are used to access a number of secure applications including campus email, the campus portal and Blackboard, the course management system used to offer courses. Network accounts are created within 24 hours of the student depositing to the University through the Office of Transfer Admissions.

The student’s initial password for their network account is compiled using a formula unique to them which incorporates information from their SJF ID number, which is provided to the student separately from the instructions to initially log in to their network account. The formula for the initial password is:

- The first letter of your PREFERRED FIRST NAME (lower case) +
- The character "!" +
- The first letter of your LAST NAME (lower case) +
- The character "$" +
- The first 2 digits of the last 4 number of your SJF ID # +
- The character " # " +
- The last 2 digits of the last 4 numbers of your SJF ID +
- The character “*” +
- The 2 digits of the birth month

Once the account is activated by the student, the network password expires every 365 days.
The requirements for a new network password are:

- Password is at least 12 characters long
- Password contains characters from at least **three** of the following categories:
    - English **uppercase** character (A-Z)
    - English **lowercase** character (a-z)
    - Numeric digits (0-9)
    - Non-alphanumeric (for example: **!**, **$**, **#**, or **%**)
    - Password does not contain three or more consecutive characters from the user’s account name

If the student forgets his/her password, they can reset it online themselves by following the directions available at https://sjfc.teamdynamix.com/TDClient/1811/Portal/KB/ArticleDet?ID=32702. If the student doesn’t know their original password, he/she may call the OIT Service Desk and the responding staff member will use three pieces of information to verify the student’s identity; SJF ID#, DOB, and mailing address.

Students will also need to enroll into Multi-Factor Authentication (MFA) to add an extra layer of protection to your network account. The instructions to enroll are available at https://sjfc.teamdynamix.com/TDClient/1811/Portal/KB/ArticleDet?ID=138388. If any issues or questions arise during this process the OIT Service Desk can be contacted for assistance.

There are currently no projected additional charges passed on to the student in the identity verification process.

OPPORTUNITIES FOR ADDITIONAL STUDENT IDENTITY VERIFICATION

All online courses at St. John Fisher University use the course management system as the main course platform. All students access the course management system with their network account each time they log in to the system, which allows them access to course materials, to submit assignments and to collaborate with their classmates synchronously or asynchronously.

In addition to the use of course management system, instructors may elect to utilize a variety of other educational technologies to ensure the identity of students in their classes.

- Online courses at St. John Fisher University are design to have a strong focus on reading, writing and project-based activities. Courses include multiple forms of assessment that allow the instructor to verify consistency in the overall tone and level of work from any individual student over the entire course term. Turnitin is available to prevent and, if necessary, identify issues of plagiarism within student work.
- If exams are given as part of an online course, there are proctoring technologies available for instructor to employ to ensure the security and integrity of the testing scenario for online delivery. This includes environmental scans of the student environment while taking a test and verification of their identity through photo id and webcam image.
- Zoom, a web conferencing technology, is available to all online courses to allow instructors and students to meet virtually using both video and audio. Instructors can utilize these interactions to verify the identity of students visually during any synchronous sessions.
- Instructors have certain information available to them about each student enrolled in their courses through the student information system, Fish'R'Net, such as address, previous enrollment and course grades and courses that were transferred from other institutions. An instructor may utilize this information to verify the identity of a specific student as needed.

St. John Fisher University, specifically the Office of Information Technology, will continuously monitor and evaluate the evolution of identity verification technologies on the market and will work to implement new technologies and procedures that are available and cost effective into the processes of the University.

RELATED POLICIES

- Academic Integrity Policy - https://www.sjf.edu/policies/academic-integrity/
- Academic Use & Privacy Policy - https://sjfc.teamdynamix.com/TDClient/1811/Portal/KB/ArticleDet?ID=34295