Guidelines for Use of External Teaching/Learning Resources

The rapidly expanding availability of web-based and other technology resources with educational applications offers opportunities for faculty to enhance student engagement and learning. Instructors may find an external resource that meets a teaching need not met by technology maintained and supported by the VSC. Faculty and staff should get approval for the use of external technology resources from IT staff as well as the Cybersecurity Team before deploying them in a course.

External Resources

Most external technology resources require students to create separate accounts, with separate logins. Apart from the inconvenience of separate logins for students and faculty, college IT staff can't access those accounts for support or troubleshooting, and they can't provide instructions for use of unfamiliar programs. External technology resources may also present security risks and FERPA / GPDR violations if they store sensitive data, such as grades.

Faculty who use external technology resources must take responsibility for training students in the use of those resources and for ensuring that sensitive data does not reside on non-VSCS systems or that an appropriate contract is in place with the vendor if sensitive data will be stored on a non-VSCS system. Increasingly, the VSC is incorporating external platforms into existing systems (an "LTI integration") while maintaining data security and the convenience of single sign-on. TurnItIn plagiarism detection, Office 365 OneDrive, Respondus Lock-Down Browser, and Badgr are examples of these LTI integrations.

The Americans with Disabilities Act (ADA) establishes requirements for the accessibility of VSC resources. All LTI integrations must be assessed for accessibility prior to adoption to ensure that they are ADA compliant.

Canvas LTI Integration Request

There are resource, usability, accessibility, and security considerations when implementing a new LTI integration (a direct connection between an external resource and Canvas). This process was created to ensure proper vetting of these integration requests. Faculty interested in making a request should first consult the VSCS Guidelines for Use of External Teaching/Learning Resources.

To request a new LTI integration, please enter a ServiceDesk ticket with the category of Canvas and the subcategory of LTI Integration. Please include details about what the resource and this integration is supposed to do, the additional functionality it will provide, and the scope of applicability of the integration (is it a resource integration desired for use across multiple curriculum areas or course sections, for example?).

The VSC Chief Academic Officer will consider the priority of the request based on the stated use case and consultation with the faculty requestor and/or relevant academic departments and deans, who will determine whether the product is ADA compliant. The request will then be passed to the VSC Cybersecurity Team to evaluate the vendor and the security of our data. If there are current contractual agreements or additional security details about the vendor in question, please provide them with the request. Finally, the VSCS Canvas Admin Team (CATs) will evaluate the product and its integration for any potential usability impact on the VSCS's configuration of Canvas. The requester will be notified of the final decision.

Managing Sensitive Data

The Vermont State Colleges have a number of operational data security policies which define "secure" and address information sensitivity, security practices, and data access security. The complete text of these policies can be found at: **https://www.vsc.edu/board-of-trustees/policies-procedures/**. All employees are responsible for adhering to these policies.

From a teaching and learning perspective there are often questions about how these policies apply to Canvas, various file portability products (the VSCS-supported Office 365 OneDrive as well as Google Drive, Dropbox, etc.), blogging tools like WordPress, and communications related to student progress and advising. Key considerations include FERPA and GDPR and the volume of data that needs to be transmitted or stored.

Data storage

Data is classified as either Private or Protected according to the VSCS Information Sensitivity Policy 627-1 (found at: https://www.vsc.edu/wp-content/uploads/2018/12/627-1-VSCS-Information-Sensitivity-Policy.pdf). Public information may be stored on any VSCS device or VSCS drive including personal and shared drives. Private information should only be stored on a VSCS desktop computer, VSCS encrypted device, VSCS personal drive, or on VSCS Microsoft OneDrive. VSCS data should not be stored on removable media or any non-VSCS device, nor should it be saved or uploaded to any non-VSCS entity, system, or vendor without a specific contract in place signed by both parties ensuring the confidentiality, integrity, and availability of VSCS data as well as compliance with FERPA, GDPR, and State of Vermont privacy laws and requirements.

Communications about a student with a third party, vendor, or contractor

To ensure compliance with FERPA and to maintain student confidentiality, the guidelines below must be followed:

- When discussing any private information via email, recipients of the communication should be limited to those with a need to know.

- Private information about any student can be sent via email or discreetly shared via phone, however, email communications must adhere to the VSCS Secure Email Transmission Policy 617-1 and the VSCS Secure Email Transmission Procedure 617-1a found at: https://www.vsc.edu/wp-content/uploads/2019/01/617-1-VSCS-Secure-Email-Transmissions-Policy.pdf and https://www.vsc.edu/wp-content/uploads/2019/01/617-1a-VSCS-Secure-Email-Transmissions-Procedure.pdf, and there must be a contractual agreement in place signed by both parties that ensure the confidentiality, integrity, and availability of VSCS data and that the third party will adhere to all FERPA, GDPR, and Vermont State privacy laws and requirements in regards to VSCS data.