

Learning Management System (LMS) Operating Procedures for Teaching and Learning Services (TLS) | For Internal Use

Table of Contents

<i>Learning Management System (LMS) Operating Procedures for Teaching and Learning Services (TLS) For Internal Use</i>	1
Purpose and Scope	3
Responsibilities & Reporting Lines	3
Definitions & Acronyms	4
User Management	4
General Access & Authentication	4
Requests for System-Wide Access	4
Administrative Bulk Access	5
Emergency Access	5
Course Lifecycle Management	6
Course Creation	6
Course Backup Responsibilities	6
Student Access to Courses	6
Course Deletion Protocols	7
Copying Course Content	7
Use of Copyrighted Materials in the LMS	7
Integration of Third-party Tools & Plugins	7
Requests.....	7
Review & Approval	7
Testing & Implementation	8
Roles & Responsibilities	8
LMS Dashboard Messaging	8
Permitted Content	8
Content Not Permitted.....	8
Submission & Approval Process	9
Data Analytics	9
Training & Support	10
System Maintenance, Outages & Upgrades	10
Planned Maintenance & Outages	10
Upgrade & Release Management.....	10
Configuration & Template Change Requests	10
Evaluation Criteria	10
Approval & Escalation Process.....	10
Appeals	11

Integrations or Customizations	11
Course Access & Other Appeals	11
Compliance & Risks	11
Accessibility	11
Risk Management	11
Incident Reporting	11
Communication & Engagement	12
Budget & Resources	12
Continuous Improvement	12
<i>Appendix A: Learning Management System (LMS) Governance Framework for Carleton University External</i>	<i>14</i>
Introduction	14
Purpose	14
Scope	14
Definitions and Acronyms	15
Principles of LMS Governance	15
Roles & Responsibilities	15
Digital Executive Committee	16
Digital Steering Committee	16
TLS Brightspace Action Team (BAT)	16
User Management	17
General Access & Authentication	17
Requests for System-Wide Access	17
Once the department head, director, or associate dean has reviewed and approved the request, they will submit the approval to TLS via the TLS Support Portal.	17
Administrative Bulk Access	17
Emergency Access	18
Course Lifecycle Management	18
Course Creation	18
Course Backup Responsibilities	19
Student Access to Courses	19
Course Deletion Protocols	19
Copying Course Content	20
Use of Copyrighted Materials in the LMS	20
Integration of Third-party Tools & Plugins	20
Data Analytics	20
Training & Support	21
Appeals	21
Integrations or Customizations	21
Course Access & Other Appeals	21
System Maintenance, Outages & Upgrades	21

Planned Maintenance & Outages	21
Upgrade & Release Management	22
Compliance & Risks	22
Accessibility	22
Risk Management.....	22
Incident Reporting.....	22
Continuous Improvement.....	23
Related Policies	23

Purpose and Scope

This document outlines Teaching and Learning Services' (TLS) responsibilities and procedures related to Carleton's learning management system (LMS). This document should be read in conjunction with the LMS Governance Framework ([Appendix A](#)) and its objectives.

The outlined responsibilities and procedures apply to all Carleton employees who support LMS-related tasks (primarily TLS staff).

Responsibilities & Reporting Lines

TLS is responsible for LMS administration and configuration, user support, training, integration vetting, verifying access for non-instructor authorized users, supports instructional needs (e.g., course design).

TLS employees triage day-to-day LMS issues and request and escalate them to the educational technology manager as needed.

The TLS educational technology manager brings forward issues requiring broader input to the TLS Brightspace Action Team (BAT), which meets monthly during the academic year.

TLS Brightspace Action Team (BAT) is responsible for the management, governance, and administration of all aspects of the LMS. This team:

- Provides operational oversight of LMS.
- Manages user interface components and design, navigation links, and tool configuration and availability.
- Manages course components including site design and structure, course codes and term designations.
- Reviews requests for system configuration changes, third-party integrations, and template adjustments.
- Evaluates proposed enhancements for usability, accessibility, and impact.
- Consults with relevant stakeholders (e.g., faculty, staff, ITS, students) during decision-making.
- Brings forward major changes to the Teaching and Learning Computing Committee (TLCC) when broader institutional impact is expected.

Definitions & Acronyms

See [LMS Glossary Table.csv](#) for additional definitions and acronyms, as they relate to the LMS.

User Management

General Access & Authentication

- All users of LMS must be authenticated with university-validated credentials (either MC1 or affiliated account).
- Requests for Affiliate accounts (for users outside Carleton University) are made by Course Creators through [Affiliate Account Request form](#).
- If the Course Creator is an academic staff member (faculty or contract instructor) and is no longer employed by Carleton University, the Dean or associate dean of the Course Creator's Faculty must approve any third-party access to course materials in LMS.
- If the Course Creator, is a non-academic staff member (including a TA), and is no longer at Carleton, their manager may be granted access to the course materials in the LMS.
- For non-MC1 accounts, the account is considered "inactive" if the users has not logged into the LMS at least once over a two-year period. Inactive accounts will be deleted on a yearly basis.
- All users, including TLS staff members, may only use the LMS for university-related purposes and must comply with the University's [Acceptable Use of Information Technology and Email Policy](#).

Requests for System-Wide Access

Initiation of Request

The requesting individual (staff, faculty, or instructor) must submit a formal request to their department head, director, or associate dean, outlining:

- The specific system-wide role requested
- The academic or administrative rationale
- Duration of access (temporary or ongoing)
- Courses, departments, or functions the access will support.

Process after Approval

Once the department head, director, or associate dean has reviewed and approved the request, they will submit the approval to TLS via the [TLS Support Portal](#). Then,

1. **BAT Review:** Approved requests will be reviewed by BAT or designated LMS system administrator.
2. **Access Provisioning:** The LMS administrator will review the request to confirm role appropriateness and ensure there is no overlap or conflict with existing access. Once confirmed, access will be provisioned and documented in the LMS access log.
3. **Notification:** The user and their supervisor will be notified once access is granted.

4. **Accountability:** Users are expected to complete any required training and adhere to LMS use, privacy, and data handling policies.
5. **Cyclical Review:** Access will be reviewed periodically and may be revoked if no longer required or if used inappropriately.

Administrative Bulk Access

- Bulk access, access to several courses in a unit, may be provided for assisting in the administration of courses within an organizational unit.
- Bulk access to LMS sites for the purposes of assisting in the administration of the course sites shall be granted at the request of the dean or designate of an academic unit, with confirmation that affected instructors have been notified.
- Bulk access shall only be granted to LMS sites for courses in the current or the following term.
- Bulk access shall not be granted to LMS sites of past term courses unless directly authorized by the instructor of record.

Emergency Access

- In cases where emergency access is necessary for a current or past course the dean or associate dean shall submit an email request to the director of TLS, who will review the request in accordance with the LMS Governance Framework.
- The dean or associate dean shall also provide suitable notification (if applicable) to the instructor.
- Depending on the reasons for emergency access to an LMS site, access to course materials, student data, and other information will follow the principle of providing only the minimum access necessary to meet the specific requirement.
- In academic courses, emergency access does **not** grant ownership of the course content in the site. Ownership rests with the copyright holder of the material regardless of access or location.

Course Lifecycle Management

Course Creation

Course Type	Process/Workflow	Notes
Academic	Automated process via an ITS script.	- Fall and Winter courses are created May 1 - Summer courses are created December 1
Continuing Education – Micro-credentials	Instructors must follow the Minor Modifications workflow through Academic Programs and Strategic Initiatives to receive approval from the Ministry of Colleges, Universities, research excellence and Security (MCURES) and Carleton University before a course shell will be created to support design and delivery of a micro-credential.	If TLS staff members receive an inquiry, they should refer instructors to Academic Programs and Strategic Initiatives (APSI) .
Continuing Education – Professional Development Training	Course Creators may undertake projects in consultation with TLS. Depending on the scope of the project, other stakeholders may need inclusion.	Fees may be charged according to the schedule in Internal Charges for Goods & Services Policy.
Non-Academic	Academic and administrative staff can submit a request for a non-academic course shell to be created for use using the Non-Academic Course Creation Request Form. These course shells may be used for staff training and development sandbox courses course shell prototyping template course shells, etc.	These courses will be deleted after two (2) years of inactivity.

Course Backup Responsibilities

- Course Creators are responsible for creating and maintaining backups for their own LMS courses.
- Upon request, TLS will provide instructions for creating backups of LMS course content.

Student Access to Courses

- Students are granted access to course materials by the instructor.

- Instructors may deactivate courses after the last day of deferred exams.
- TLS will deactivate courses 18 months after the course end date.
- Instructors may re-activate their courses after this time should they wish to provide students with ongoing access.

Course Deletion Protocols

- Course content will be archived for five years in alignment with the LMS Data Retention Policy.
- If exceptional circumstances require deleting academic courses before the end of the five-year retention period, written requests must be submitted to TLS by the appropriate dean.
- Retrieval of course materials will not be possible once courses and course content have been deleted.

Copying Course Content

- For academic courses, TLS will **not** copy course content to another course without the express written consent of the Course Creator.
 - This does not apply for courses/programs where the LMS courses are owned/licensed by the university (e.g., Sprott OMBA).
- If the Course Creator is not available, a dean, associate dean (for academic courses), director or department head (for non-academic courses) must make a formal request for course copying.

Use of Copyrighted Materials in the LMS

- Course Creators are responsible for ensuring that course content complies with the Carleton University Fair Dealing Policy.
- TLS staff members may advise course creators to link course materials via the university library resource system (e.g., ARES) whenever possible.
- Copyrighted material posted to the LMS may be subject to periodic review by the Office of the University Secretariat.

Integration of Third-party Tools & Plugins

Requests

All requests must be submitted at least one semester in advance of intended use via the [Integration Request Form](#).

License fees for third-party tools are not responsibility of TLS, and any fees must follow university policy.

Review & Approval

All requests are reviewed by TLS, BAT, the LMS Administrator, and the EdTech Manager with input from relevant university offices. The review includes:

- Evaluation of vendor-provided accessibility and security documentation (e.g., VPAT, HECVAT).

- Confirmation that the tool meets Carleton's integration standards (currently LTI 1.3 with limited direct API access).
- Consultation with Privacy and Security teams as needed.

Testing & Implementation

If the request is conditionally approved:

- The requestor will participate in testing to ensure the integration functions as intended.
- The integration will not be finalized until testing is complete and all standards are met.

Roles & Responsibilities

- **Requestor:** May be responsible for vendor fees and must support functional testing.
- **Vendor:** Responsible for end-user support related to the tool itself.
- **TLS:** Supports LMS-side implementation, coordinates, review, and ensures alignment with institutional policies and LMS Governance Framework.

LMS Dashboard Messaging

The LMS dashboard messaging area is intended primarily for critical, time-sensitive, and technical information that directly impacts the user's ability to access or utilize the learning environment.

Permitted Content

Messages permitted on the main dashboard announcements section must be directly relevant to the current academic community (students, faculty, and staff) and fall strictly into one of the following three categories:

1. **Technical stability and access.** Announcements about the operational status of the LMS or integrated tools (e.g., scheduled maintenance notice, system outages, security updates, version requirements)
2. **Critical academic deadlines.** Time-sensitive, high-importance reminders for all users that affect core teaching and learning function (e.g., course registration, withdrawal deadlines, final grade submission periods, start/end of term notice).
3. **Urgent safety and security announcements.** Messages regarding immediate threats or mandatory actions related to user data or physical safety on campus (e.g., system compromise alert, mandatory password reset requirements, extreme weather/campus closure notifications (only if other channels fail), active shooter on campus).

Content Not Permitted

The following types of content are strictly excluded from the LMS dashboard to avoid clutter, maintain focus, and prevent the dashboard from becoming a general marketing channel:

- **General advertising/marketing.** Promoting non-essential services, sales, external events, or commercial offerings (e.g., bank promotions, local business discounts).
- **Non-urgent events and activities.** Announcements for clubs, social events, workshops, or non-mandatory training (e.g., departmental or student events, department picnics, optional career fairs).
- **General information posts.** Messages that can be communicated through other official channels (e.g., email, university news site, social media).
- **Surveys and research calls.** Requests for participation in academic research studies or non-mandatory institutional surveys.
- **Updates to policies.** Updates to policies that do not directly affect the user's ability to log in or use core learning environment functions (e.g., general HR policy updates).

Submission & Approval Process

Submission: All requests for dashboard postings must be submitted to the [TLS Support portal](#) at least 48 hours prior to the requested posting time.

Format: Messages must be written in full by the requestor. They must be concise, written clearly, and state the immediate action required or the impact on the user.

Duration: Postings will be limited to a maximum of 48 hours unless it is a multi-day event like a scheduled maintenance window.

Final Authority: BAT holds the final authority on all content posted to the LMS dashboard.

Data Analytics

Access to [built-in learning analytics tools in Brightspace](#) to conduct university business is subject to relevant university policies, including the Freedom of Information and Protection of Privacy Act (FIPPA), the Acceptable Use of IT and Email Policy, the Responsible Conduct of Research Policy, and Research Ethics Board guidelines.

- Data requests related to LMS usage (e.g., course activity, login frequency, tool adoption) must be submitted through the [TLS Support Portal: Learning Analytics Request](#).
- Instructors and course managers may use available course-level reports to support student success. TLS provides guidance and training to ensure analytics are used responsibly, with a focus on improving learning outcomes rather than monitoring individuals.
- LMS Analytics may also be used to support research. Before any information (obtained from the LMS) can be used for scholarly research purposes, it must first be approved by relevant university's Research Ethics Boards (A or B).

Training & Support

Brightspace training opportunities for Course Creators, Teaching Assistants, and Administrative Staff are listed on [Carleton's Brightspace Training](#) site. Training for specific departments is also available upon request.

Brightspace support is available through TLS' [Brightspace Support Site](#).

LMS users can submit support requests via [TLS Support Portal](#).

System Maintenance, Outages & Upgrades

Planned Maintenance & Outages

- TLS will notify all Authorized Users in advance of any scheduled LMS maintenance or service disruptions. Outages are scheduled to minimize impact and avoid peak instructional periods when possible.
- It is the responsibility of Teaching Staff and other users to review posted notifications and plan assessments accordingly.

Upgrade & Release Management

D2L Brightspace operates on a continuous release cycle, which ultimately reduces the need for planned outages. TLS evaluates and approves feature updates prior to deployment. For details on how releases are reviewed, tested, and communicated, see the [Brightspace Release Management and Approval Process](#).

Governance decisions related to LMS configuration, templates, and system-wide enhancements follow a structured review and approval process led by BAT.

Configuration & Template Change Requests

Requests to modify LMS templates or settings must be submitted to the BAT team in writing. Approved changes must adhere to accessibility and usability best practices.

Evaluation Criteria

When reviewing proposed changes or enhancements, BAT considers:

- Compliance requirements (e.g., AODA, FIPPA, institutional policies)
- Impact on user workflows (faculty, students, administrators)
- Change management implications (training, documentation, support needs)
- Alignment with the LMS roadmap and institutional priorities
- Whether the request addresses a known gap or solves a defined problem.

Note: Opting out of mandatory updates (e.g., for security or accessibility) is not permitted.

Approval & Escalation Process

- BAT conducts an initial investigation to assess feasibility and stakeholder impact.

- Security or risk assessments are required when data exchange or third-party licensing is involved.
- AODA compliance is a legal requirement for all approved changes.
- Once a decision is made, the requestor is notified with a rationale and an estimated timeline for implementation.

Appeals

Integrations or Customizations

Where a request for an integration has been denied, a complainant may submit a written request for review to the director of TLS or designate with rationale for the appeal.

Course Access & Other Appeals

Where a request to access a course has been denied, a complainant may submit a written request for review to the director of TLS or designate with rationale for the appeal. The Vice-Provost (Academic & Global Learning) may grant or deny access.

If a course owner believes that access to their content has been inappropriately provided by any staff member of TLS, they may submit a description of the issue via the [TLS Support Portal](#). TLS will work with the site owner toward a satisfactory resolution.

If the situation is not fully resolved, complainants may contact the relevant dean or designate and submit a written complaint.

If the situation is still not fully resolved, complainants may submit a written complaint to the Vice-Provost (Academic & Global Learning) or designate.

Compliance & Risks

Accessibility

Accessibility awareness training related to the development of accessible course delivery and instruction is available on the TLS website.

Risk Management

TLS actions include:

- Monitoring system uptime and vendor performance to ensure consistent platform availability.
- Managing third-party integrations and minimizing dependency risks.
- Coordinating with D2L and ITS to address incidents, vulnerabilities, or disruptions.

Incident Reporting

Incidents affecting the LMS (e.g., system downtime, service outages, security or data incidents, unintended system-level changes) must be reported and addressed promptly through established reporting channels:

- Users submit incidents via the TLS Support Portal, which feeds directly into our Jira Service Management system for triaging and resolution.
- TLS Staff escalate the issue accordingly (e.g., system administrator, manager, D2L vendor, EUS support).

All incidents are logged, tracked, and reviewed for patterns or risks. TLS communicates major incidents and resolutions through the LMS system announcements, direct emails to affected users (as needed), and updates via the TLS and Brightspace websites.

Communication & Engagement

Type of Communication	Details	Vehicle(s) of Communication
Stakeholder	Major updates (e.g., feature changes, outages, policy shifts)	• LMS system announcements • TLS newsletter • Direct email to affected user groups
Feedback and Collaboration	TLS engages instructors and students	• Surveys (e.g., mid-year LMS survey) • Consultation sessions (e.g., with BAT, faculty reps) • Focus groups and pilot testing
Framework	Governance changes	• Published on the TLS and Brightspace websites • Announced via LMS news and departmental mailing lists

Budget & Resources

Funding for the LMS license is included in the university budget (UB) and like other enterprise software license is administered by ITS as directed by the Office of the Vice Provost (Academic and Global Learning).

TLS supports the budget planning process and contributes significant human capital resources in terms of support, testing, integration, administration, and planning.

Resource planning for LMS administration and support is led by the educational technology manager in consultation with the TLS management team. It includes staffing; infrastructure; support hours and coverage; service continuity; and risk mitigation.

Continuous Improvement

TLS reviews LMS use annually through internal audits, Brightspace analytics, and stakeholder feedback.

New tools and features are piloted with volunteer instructors and reviewed for scalability and accessibility.

Data from service requests, feedback surveys, and BAT discussions inform decisions on changes to tools, support, and training.

Appendix A: Learning Management System (LMS) Governance Framework for Carleton University | External

Introduction

A learning management system (LMS) provides organized, consistent, and timely course-related communication between instructors and students. The use of an LMS is intended to assist instructors with course administration while supporting student engagement, increasing flexible learning opportunities, and enabling quality-learning experiences. An LMS provides an efficient and effective vehicle for ongoing student feedback.

Purpose

This document outlines Carleton University's governance framework for the use of its LMS, supporting academic delivery and institutional accountability and compliance with Carleton University policies.

The objectives of the framework are to:

- **Ensure Academic and Pedagogical Integrity.** Support high-quality teaching, learning, and assessment across all modalities (e.g., in person, blended, online).
- **Promote Equitable Access and Support.** Provide accessible user experiences, training, and documentation for all stakeholders.
- **Uphold Data Privacy and Regulatory Compliance.** Align operations with institutional policies and standards, including Freedom of Information and Protection of Privacy Act (FIPPA), Accessibility for Ontarians with disabilities Act (AODA), and Web Content Accessibility Guidelines (WCAG).
- **Foster Sustainable and Scalable Operations.** Maintain platform performance and manage system updates and resources responsibly.
- **Enable Inclusive and Transparent Decision-Making.** Include faculty, staff, students, and service units in governance processes.
- **Support Innovation and Continuous Improvement.** Encourage evidence-based experimentation and the thoughtful adoption of new tools and practices.

Scope

This framework applies to all credit and non-credit courses delivered through Carleton University's LMS. It is intended for:

- Academic and administrative staff who manage or support LMS content.
- Students engaging with LMS-based learning experiences.
- External tools and systems officially integrated with the LMS.

It does NOT apply to third-party platforms that are not institutionally supported or integrated.

The framework supports compliance with privacy and accessibility requirements and ensures alignment with Carleton's digital learning strategy.

Definitions and Acronyms

See [LMS Glossary Table.csv](#) for additional definitions and acronyms, as they relate to the LMS.

Principles of LMS Governance

The LMS governance objectives outlined above guide how decisions are made, roles are defined, and resources are allocated. Governance is grounded in principles of equity, transparency, and compliance, and is implemented through the structure and stakeholder responsibilities detailed below.

Roles & Responsibilities

Stakeholder	Primary Responsibilities
Teaching and Learning Services (TLS)	LMS administration and configuration, user support, training, integration vetting, verifying access for non-instructor Authorized Users, supports instructional needs (e.g., course design)
Information Technology Services (ITS)	SIS integration, data sync, account provisioning
Course Creators	Course content, AODA and copyright compliance, follow Acceptable Use, FIPPA, Academic Integrity, and Email policies, store backup of course materials, empower students to monitor progress in the LMS, file management
Scheduling and Examination Services (SES)	Supports formerly scheduled exam configuration
Library	Guidance on (and support with) linking ARES materials
Paul Menton Centre for Students with Disabilities (PMC)	Guidance on (and support with) accessibility of materials
Registrar's Office	Releases academic course shells

Students

Follow Acceptable Use, Academic Integrity, and Email policies

Digital Executive Committee

- Ensures alignment of initiatives with the strategic priorities of the university.
- Identifies and recommends levels of investment and funding in IT.
- Sets and communicates the overall business objectives as they relate to IT.

Final authority for LMS governance rests with this committee.

Digital Steering Committee

- Guides the strategic directions and priorities of IT as they relate to the business of the university and ensure alignment with the Strategic Integrated Plan and the Digital Strategy,
- Approves and guides strategic decisions regarding LMS that may impact most of the university community or have significant financial impacts (e.g., procurement of a new LMS).

Teaching, Learning, Technology Committee (TLTC)

- Serves as the institutional advisory body on teaching and learning technologies,
- Reviews and endorses strategic decisions related to LMS policy, adoption, and large-scale changes.
- Provides direction on university-wide LMS priorities and alignment with academic goals.
- Forwards reports/updates, recommendations as required to Digital Steering Committee, particularly regarding resourcing or strategic implications.

All strategic decisions that affect policy, funding, or institutional direction are reviewed by this committee.

TLS Brightspace Action Team (BAT)

- Provides operational oversight of LMS.
- Manages user interface components and design, navigation links, and tool configuration and availability.
- Manages course components including site design and structure, course codes and term designations.
- Reviews requests for system configuration changes, third-party integrations, and template adjustments.
- Evaluates proposed enhancements for usability, accessibility, and impact.
- Consults with relevant stakeholders (e.g., faculty, staff, ITS, students) during decision-making.
- Brings forward major changes to the Teaching and Learning Computing Committee (TLCC) when broader institutional impact is expected.

User Management

General Access & Authentication

- All users of LMS must be authenticated with university-validated credentials (either MC1 or affiliated account).
- Requests for Affiliate accounts (for users outside Carleton University) are made by Course Creators through [Affiliate Account Request form](#).
- If the Course Creator is an academic staff member (faculty or contract instructor) and is no longer employed by Carleton University, the Dean or associate dean of the Course Creator's Faculty must approve any third-party access to course materials in LMS.
- If the Course Creator, is a non-academic staff member (including a TA), and is no longer at Carleton, their manager may be granted access to the course materials in the LMS.
- For non-MC1 accounts, the account is considered "inactive" if the users has not logged into the LMS at least once over a two-year period. Inactive accounts will be deleted on a yearly basis.
- All users, including TLS staff members, may only use the LMS for university-related purposes and must comply with the University's [Acceptable Use of Information Technology and Email Policy](#).

Requests for System-Wide Access

Initiation of Request

The requesting individual (staff, faculty, or instructor) must submit a formal request to their department head, director, or associate dean, outlining:

- The specific system-wide role requested
- The academic or administrative rationale
- Duration of access (temporary or ongoing)
- Courses, departments, or functions the access will support.

Process after Approval

Once the department head, director, or associate dean has reviewed and approved the request, they will submit the approval to TLS via the [TLS Support Portal](#).

Administrative Bulk Access

- Bulk access, access to several courses in a unit, may be provided for assisting in the administration of courses within an organizational unit.

- Bulk access to LMS sites for the purposes of assisting in the administration of the course sites shall be granted at the request of the dean or designate of an academic unit, with confirmation that affected instructors have been notified.
- Bulk access shall only be granted to LMS sites for courses in the current or the following term.
- Bulk access shall not be granted to LMS sites of past term courses unless directly authorized by the instructor of record.

Emergency Access

- In cases where emergency access is necessary for a current or past course the dean or associate dean shall submit an email request to the director of TLS, who will review the request in accordance with the LMS Governance Framework.
- The dean or associate dean shall also provide suitable notification (if applicable) to the instructor.
- Depending on the reasons for emergency access to an LMS site, access to course materials, student data, and other information will follow the principle of providing only the minimum access necessary to meet the specific requirement.
- In academic courses, emergency access does **not** grant ownership of the course content in the site. Ownership rests with the copyright holder of the material regardless of access or location.

Course Lifecycle Management

Course Creation

Course Type	Process/Workflow	Notes
Academic	Automated process via an ITS script.	• Fall and Winter courses are created May 1 • Summer courses are created December 1
Continuing Education – Micro-credentials	Instructors must follow the Minor Modifications workflow through Academic Programs and Strategic Initiatives to receive approval from the Ministry of Colleges, Universities, research excellence and Security (MCURES) and Carleton University before a course shell will be created to support design and delivery of a micro-credential.	If TLS staff members receive an inquiry, they should refer instructors to Academic Programs and Strategic Initiatives (APSI) .
Continuing Education – Professional	Course Creators may undertake projects in consultation with TLS. Depending on the scope of the	Fees may be charged according to the schedule in Internal Charges for Goods & Services Policy.

Development Training	project, other stakeholders may need inclusion.	
Non-Academic	Academic and administrative staff can submit a request for a non-academic course shell to be created for use using the Non-Academic Course Creation Request Form. These course shells may be used for staff training and development sandbox courses course shell prototyping template course shells, etc.	These courses will be deleted after two (2) years of inactivity.

Course Backup Responsibilities

- Course Creators are responsible for creating and maintaining backups for their own LMS courses.
- Upon request, TLS will provide instructions for creating backups of LMS course content.

Student Access to Courses

- Students are granted access to course materials by the instructor.
- Instructors may deactivate courses after the last day of deferred exams.
- TLS will deactivate courses 18 months after the course end date.
- Instructors may re-activate their courses after this time should they wish to provide students with ongoing access.

Course Deletion Protocols

- Course content will be archived for five years in alignment with the LMS Data Retention Policy.
- If exceptional circumstances require deleting academic courses before the end of the five-year retention period, written requests must be submitted to TLS by the appropriate dean.
- Retrieval of course materials will not be possible once courses and course content have been deleted.

Copying Course Content

- For academic courses, TLS will **not** copy course content to another course without the express written consent of the Course Creator.
 - This does not apply for courses/programs where the LMS courses are owned/licensed by the university (e.g., Sprott OMBA).
- If the Course Creator is not available, a dean, associate dean (for academic courses), director or department head (for non-academic courses) must make a formal request for course copying.

Use of Copyrighted Materials in the LMS

- Course Creators are responsible for ensuring that course content complies with the Carleton University Fair Dealing Policy.
- TLS staff members may advise course creators to link course materials via the university library resource system (e.g., ARES) whenever possible.
- Copyrighted material posted to the LMS may be subject to periodic review by the Office of the University Secretariat.

Integration of Third-party Tools & Plugins

Third-party tools and services may be integrated into the LMS to enhance teaching and learning. These integrations must meet institutional standards for accessibility, privacy, and security.

All requests must be submitted at least one semester in advance of intended use via the [Integration Request Form](#).

License fees for third-party tools are not responsibility of TLS, and any fees must follow university policy.

Data Analytics

Access to [built-in learning analytics tools in Brightspace](#) to conduct university business is subject to relevant university policies, including the Freedom of Information and Protection of Privacy Act (FIPPA), the Acceptable Use of IT and Email Policy, the Responsible Conduct of Research Policy, and Research Ethics Board guidelines.

- Data requests related to LMS usage (e.g., course activity, login frequency, tool adoption) must be submitted through the [TLS Support Portal: Learning Analytics Request](#).
- Instructors and course managers may use available course-level reports to support student success. TLS provides guidance and training to ensure analytics are used responsibly, with a focus on improving learning outcomes rather than monitoring individuals.

- LMS Analytics may also be used to support research. Before any information (obtained from the LMS) can be used for scholarly research purposes, it must first be approved by relevant university's Research Ethics Boards (A or B).

Training & Support

Brightspace training opportunities for Course Creators, Teaching Assistants, and Administrative Staff are listed on [Carleton's Brightspace Training](#) site. Training for specific departments is also available upon request.

Brightspace support is available through TLS' [Brightspace Support Site](#).

LMS users can submit support requests via [TLS Support Portal](#).

Appeals

Integrations or Customizations

Where a request for an integration has been denied, a complainant may submit a written request for review to the director of TLS or designate with rationale for the appeal.

Course Access & Other Appeals

Where a request to access a course has been denied, a complainant may submit a written request for review to the director of TLS or designate with rationale for the appeal. The Vice-Provost (Academic & Global Learning) may grant or deny access.

If a course owner believes that access to their content has been inappropriately provided by any staff member of TLS, they may submit a description of the issue via the [TLS Support Portal](#). TLS will work with the site owner toward a satisfactory resolution.

If the situation is not fully resolved, complainants may contact the relevant dean or designate and submit a written complaint.

If the situation is still not fully resolved, complainants may submit a written complaint to the Vice-Provost (Academic & Global Learning) or designate.

System Maintenance, Outages & Upgrades

Planned Maintenance & Outages

- TLS will notify all Authorized Users in advance of any scheduled LMS maintenance or service disruptions. Outages are scheduled to minimize impact and avoid peak instructional periods when possible.
- It is the responsibility of Teaching Staff and other users to review posted notifications and plan assessments accordingly.

Upgrade & Release Management

D2L Brightspace operates on a continuous release cycle, which ultimately reduces the need for planned outages. TLS evaluates and approves feature updates prior to deployment. For details on how releases are reviewed, tested, and communicated, see the [Brightspace Release Management and Approval Process](#).

Governance decisions related to LMS configuration, templates, and system-wide enhancements follow a structured review and approval process led by BAT.

Compliance & Risks

Accessibility

Carleton University is committed to providing all users equitable access to course materials placed in the LMS.

AODA standards have been considered in the development of this document and it adheres to the principles outlined in the university's [AODA Multi-Year Accessibility Plan](#).

Accessibility awareness training related to the development of accessible course delivery and instruction is available on the TLS website.

Risk Management

This framework adheres to the University's [Data Protection and Risk Management Policy](#) to ensure the LMS is secure, compliant, and reliable.

Risk governance includes:

- Monitoring system uptime and vendor performance to ensure consistent platform availability.
- Managing third-party integrations and minimizing dependency risks.
- Coordinating with D2L and ITS to address incidents, vulnerabilities, or disruptions.

Incident Reporting

Incidents affecting the LMS (e.g., system downtime, service outages, security or data incidents, unintended system-level changes) must be reported and addressed promptly through established reporting channels:

- Users submit incidents via the TLS Support Portal, which feeds directly into our Jira Service Management system for triaging and resolution.
- TLS Staff escalate the issue accordingly (e.g., system administrator, manager, D2L vendor, EUS support).

All incidents are logged, tracked, and reviewed for patterns or risks. TLS communicates major incidents and resolutions through the LMS system announcements, direct emails to affected users (as needed), and updates via the TLS and Brightspace websites.

Continuous Improvement

TLS reviews LMS use annually through internal audits, Brightspace analytics, and stakeholder feedback.

New tools and features are piloted with volunteer instructors and reviewed for scalability and accessibility.

Related Policies

(All policies are available at the [University Secretariat website](#))

- Acceptable Use of Information Technology and Email Policy
- Access to Information and Privacy Policy
- Accessibility for Ontarians with disabilities Act (AODA)
- Carleton University Fair Dealing Policy
- Corporate Records and Archive Policy
- Data Protection and Risk Management Policy
- Electronic Monitoring Policy
- Freedom of Information and Protection of Privacy Act (FIPAA)
- Responsible Conduct of Research Policy
- Retention and Removal of Course Related Data in LMS Policy
- University Information Technology (IT) Security Policy