Online Driver Training Course

Requirements for Approval

In addition to meeting and/or exceeding course standards for the specified type of driver training, driver training schools who offer online driver training must also meet the following criteria for the approval of an online driver training course.

1. Driver training schools must provide unlimited access to Alberta Transportation, DEES, to participate in the Online Driving Course and access to administrative functions of the Online Driving Course as a condition of approval and once approval has been granted, for auditing purposes only.

2. In order to be approved to deliver online driver training the driver training school must have offered driver training in-person for a minimum of 2 years and must be in good standing with DEES within the 2 year period.

3. Course content must meet minimum hours for the specified type of driver training. The minimum course hours is based on time required to teach an instructional component and is exclusive of supplemental material or the time it takes the student to complete each component.

4. Instructor facilitates the course using one of the two methods:
    - Instructor-led: the online instructor leads the course through face-to-face or other interactive methods (i.e. phone). The instructor interacts with students regularly and actively monitors student progress.
    - Instructor-monitored/supported: an online instructor monitors the online course, student progress, reviews and assesses learner submissions as required, and answers questions or concerns in a timely manner.
    - Instructor contact information and hours of availability must be provided to the student.

5. Technical requirements such as hardware, software, internet connection speed, and other components needed to take the course are clearly stated on the driver training school website prior to registration of the course.

6. Considerations must be made for areas with low bandwidth.

7. The course should be browser and OS independent (i.e., IE, Chrome, Firefox, or Safari on Windows or Mac).

8. Technical support for must be available to students. Contact information and hours of availability for technical support must be provided to the student.

9. The student is logged out of the course after a specified time of inactivity and must login to resume the course.

10. The identity of the student is verified on a random basis throughout the course to ensure the student who is signed in is the individual completing the course (e.g., the student is prompted with security questions upon at random during the course).

11. Online courses must illustrate course objectives and key components using multiple media formats such as text, audio, illustration, simulations, images or interactive graphics. Examples of different types of media include: diagrams, tables, charts, videos, comic strips, photos, virtual manipulation, and animation.

12. Course must be supported by an option to have audio-narrative enhancement of the course content, including module assessments and final exam.

13. Course must be supported by an option to have close captioning of the course content.

14. Online course must require student engagement or interaction with the course content. A minimum of three (3) levels of interactivity must be integrated into the program. Examples of this are:
    a. Interactive activities;
    b. Bulletin board; or
    c. Use interactive web tools for communication with administrative support staff or driving instructor(s) (e.g. chats or discussion forums within the course application).

15. Student must have multiple means of navigating through information in each module.

16. Course must have options for different methods of responding to activities and navigation through course content such as: using a mouse, keyboard, voice, and hand.

17. Course must include a method students can use to monitor their progress through the course and each module. For example, a progress bar or checklist of topics or activities to be completed by the student and the student's current completion status.

18. Student must not be permitted to navigate through the course without covering the information on each screen in each module.

19. The end of each module must have at least one type of student assessment that measures the extent to which students have met the learning objectives within each module.

    Examples of online assessment methods include:
    a. Multiple choice
    b. true/false
    c. fill-in-the-blank
    d. flash cards
    e. games

    - Student must successfully complete all module assessments in order to progress to the next module;
    - Students must achieve a minimum of grade of 80% on module assessments; and
    - Multiple choice, true/false, fill-in-the-blank module assessments must have a minimum of 10 questions.

20. Student must sign disclosure statement and warning at the completion of the driver training course and prior to attempting the final examination.

Disclosure Statement and Warning

WARNING to student – Any false or misleading statement on this form, including concealment of any material fact, may invalidate the results of the course and examination and may be grounds for criminal prosecution.

1. I _____ and only I, have completed this online driving course.
2. I _____ am the individual that will be attempting the final exam. My operator licence number is _____.

DECLARATION – I solemnly declare that the statements made in this declaration are true. I declare that I have read and understood the **WARNING to student.** I agree that I may be contacted by Alberta Transportation regarding this course and examination.

21. Prior to the completion of course registration, students must be informed that personal information provided by the student to enroll in the driver training course is collected under the authority of the Personal Information Protection Act of Alberta (PIPA).
    a. Students must also be informed that the requested personal information is necessary for the registration and administration of this training session and may be used for program evaluation of the driver training course.
    b. Students must be given a reasonable opportunity to accept or decline his or her consent.
    c. The driver training school must develop policies and practices to protect personal information collected from students. This privacy policy must provided to or be made accessible to the student.

22. Driver training schools must take reasonable security measures to protect personal information collected. PIPA does not specify particular security safeguards, however, driver training schools must continually ensure security measures are up-to-date to protect personal information as technologies evolve and new risks emerge. Technological tools and physical measures can include:

Software

1. Authentication
    - Users are required to login the course using two-factor authentication
    - Use of security questions as an additional layer of security when multi-factor authentication is not available.

2. User access should be role based and privileged IDs should have access to that data required to perform their job function.

3. Passwords
    - Transmitted and stored in a secure manner.
    - Encrypted using SSL
    - Password length and complexity requirements (min 8 characters, at least one upper case and one numeric or other allowed symbols).

- Password entry is obstructed on the user's screen. For example, the password is displayed as "********"
- Account disabling after an established number of invalid login attempts.
- After an account is disabled due to invalid login attempts, it is locked and the student must contact administration for password reset.
- When a password is changed, the existing password must be entered prior to accepting a new password
- When the user forgets a password, the password must be changed and not "recovered". Passwords must not be stored in a way that would allow recovery.
- All authentication attempts (log in, log out, failed logins, and password change requests should be logged and available for auditing upon request.

4. Network traffic must be secure with a minimum SSL 128 bit encryption.

5. Online course uses current SSL encryption certificate from a global trusted organization to protect the student from any malicious activities from hackers

6. The course should not require files or data to be stored on the client side (person taking the course on their home computer).

7. The course may use encrypted "cookies" to maintain connection. Cookies must not contain or be used to obtain sensitive information, such as the user ID or password. All cookies and any session information must be cleared automatically upon exit of the training program.

8. Maintain and monitor logs.
    - Log all authentication and authorization events, administrator activity, deletion of data, server-side input validation failures.
    - Logs should provide sufficient details to identify suspicious or malicious activity (i.e. date time, initiating process, process owner, and description).
    - Logs are monitored and audited on a regular basis.

Hardware

1. All content resides on a secure dedicated server located in Canada. Organizations who use a service provider outside of Canada for the collection, use, or disclosure of personal information to must abide by PIPA guidelines:
    a. The driver training school privacy policies and practices must include the country where the information is retained and the purpose(s) for which the service provider is authorized to collect use or disclose the information.
    b. The student must be informed of how they can obtain access to policies and practices with respect to the service provider.
    c. The student must be informed of the name and title of a contact person who is able to answer questions related to the service provider.
2. Full server back-up protection.
3. Protection against power outages and surges.
4. Server(s) hosted on premise is (are) located in a specially designed server room with high security and protection.

5. Security procedures against theft and hackers.
6. Network Administrators on duty 24 hours, 7 days a week.

It is highly recommended that the operational procedures and environment should adhere to web application security best practices.

Additional information on PIPA can be viewed at https://www.alberta.ca/personal-information-protection-act.aspx