Scenario: Evaluating ChatGPT Enterprise for "Learn-a-Lot!"

Nonprofit: *Learn-a-Lot!,* a nonprofit dedicated to providing quality after-school education for underserved communities.

Objective: *Learn-a-Lot!* is considering using OpenAI's ChatGPT Enterprise to support educators in developing customized lesson plans, saving time and generating creative ideas to enhance student learning. To ensure the tool aligns with its mission and complies with data security, privacy, and ethical guidelines, *Learn-a-Lot!* needs to evaluate OpenAI's terms and policies.

Part I: Worksheet – Evaluating OpenAI Terms

Instructions: Using the [OpenAI Terms & Policies](#), answer the following questions to determine whether ChatGPT Enterprise meets *Learn-a-Lot!*'s standards for data privacy, accuracy, and responsible AI use. These questions help assess compliance, ownership, and risk management to ensure safe use of AI in lesson planning.

1. **Data Ownership, Usage, and Privacy**

Description: *Learn-a-Lot!* needs to understand how data is handled within ChatGPT to ensure the security and privacy of educational content and compliance with regulations like FERPA. The goal is to confirm data rights and limitations on data use by OpenAI, including any rights to data inputs or outputs generated during lesson planning.

- **How does OpenAI handle data submitted to ChatGPT Enterprise? What rights does it have to access and use this data?**

  Our Obligations for Customer Content. We will process and store Customer Content in accordance with our Enterprise privacy commitments. We will only use Customer Content as necessary to provide you with the Services, comply with applicable law, and enforce OpenAI Policies. We will not use Customer Content to develop or improve the Services. ([Business Terms](#); 3.2)

  Our Security Program. We will maintain an information security program (including the adoption and enforcement of internal policies and procedures) designed to (a) protect the Services and Customer Content against accidental or unlawful loss, access, or disclosure, (b) identify reasonably foreseeable and internal risks to security and unauthorized access, and (c) minimize security risks, including through regular risk assessments and testing. ([Business Terms](#); 5.1)

  Our Security Obligations. As part of our information security program, we will: (a) implement and enforce policies related to electronic, network, and physical monitoring and data storage, transfer, and access; (b) deploy production infrastructure behind VPNs where possible; (c) require multi-factor authentication for employees; (d) configure network security, firewalls, accounts, and resources for least-privilege access; (e) maintain a logging and incident response process; (f) maintain corrective action plans to

respond to potential security threats; and (g) conduct periodic reviews of our security and the adequacy of our information security program as aligned to industry best practices and our own policies and procedures. ([Business Terms](#); 5.2)

Does OpenAI train its models on my business data?
By default, we do not use your business data for training our models. If you have explicitly opted in to share your data with us (for example, through our opt-in feedback mechanisms(opens in a new window)) to improve our services, then we may use the shared data to train our models. ([Enterprise Privacy Policy](#))

Does OpenAI review my business data?
We may run any business data submitted to OpenAI's services through automated content classifiers and safety tools, including to better understand how our services are used. The classifications created are metadata about the business data but do not contain any of the business data itself. Business data is only subject to human review as described below on a service-by-service basis. ([Enterprise Privacy Policy](#))

Who can view conversations and chat history in ChatGPT Enterprise and ChatGPT Edu?
Within your organization, end users can view their own conversations. Your organization has control over workspaces, and workspace admins can access an audit log of conversations and GPTs through the Enterprise Compliance API(opens in a new window). Authorized OpenAI employees will only ever access your conversations for the purposes of resolving incidents, recovering end user conversations with your explicit permission, or where required by applicable law. ([Enterprise Privacy Policy](#))

How does OpenAI ensure data security?
OpenAI encrypts all data at rest (AES-256) and in transit between our customers and us and between us and our service providers (TLS 1.2+), and uses strict access controls to limit who can access data. Our security team has an on-call rotation that has 24/7/365 coverage and is paged in case of any potential security incident. We offer a Bug Bounty Program for responsible disclosure of vulnerabilities discovered on our platform and products. Please visit our [Trust Portal](#) (opens in a new window) for more details. ([Enterprise Privacy Policy](#))

- o Evaluation:

2. **Risk Allocation**

Description: ChatGPT might occasionally provide inaccurate information or generate outputs that infringe a third party's IP rights. *Learn-a-Lot!* needs to assess OpenAI's limitations on liability and indemnification to understand the extent to which OpenAI protects users from liability caused by its services and the outputs they generate.

- ● **What limitations has OpenAI placed on its liability?**

  Limitation of Liability

11.1 Limitations on Indirect Damages. Except for (i) a party's gross negligence or willful misconduct, (ii) your breach of Section 2 (Restrictions), (iii) either party's breach of its confidentiality obligations under Section 4 (Confidentiality), (iv) our breach of Section 5 (Security), or (v) a party's indemnification obligations under this Agreement, neither you nor OpenAI or our respective affiliates or licensors will be liable under this Agreement for any indirect, punitive, incidental, special, consequential, or exemplary damages (including lost profits) even if that party has been advised of the possibility of those damages.

11.2 Liability Cap. Except for (i) a party's gross negligence or willful misconduct or (ii) a party's indemnification obligations under this Agreement, each party's total liability under the Agreement will not exceed the total amount you have paid to us in the twelve (12) months immediately prior to the event giving rise to liability. The foregoing limitations will apply despite any failure of essential purpose of any limited remedy and to the maximum extent permitted under applicable law.

([Business Terms](#))

  o   Evaluation:

- **Does OpenAI cover indemnification for IP infringement of outputs generated by the AI tool? What is excluded from this indemnification?**

  OpenAI's indemnification obligations to ChatGPT Enterprise customers under the Agreement include claims that Customer's use or distribution of Output infringes a third party's intellectual property right. This indemnity does not apply where: (i) Customer or Customer's End Users knew or should have known the Output was infringing or likely to infringe, (ii) Customer or Customer's End Users disabled, ignored, or did not use any relevant citation, filtering or safety features or restrictions provided by OpenAI, (iii) Output was modified, transformed, or used in combination with products or services not provided by or on behalf of OpenAI, (iv) Customer or its End Users did not have the right to use the Input or fine-tuning files to generate the allegedly infringing Output, (v) the claim alleges violation of trademark or related rights based on Customer's or its End Users' use of Output in trade or commerce, and (vi) the allegedly infringing Output is from content from a Third Party Offering. ([Service Terms](#); 3b)

  o   Evaluation:

3. **Chat GPT Use Restrictions**

Description: *Learn-a-Lot!* is interested in potentially exploring additional ways to leverage the lesson plans created by ChatGPT Enterprise, including by using these to train a custom AI model. Before doing so, *Learn-a-Lot!* needs to ensure these future uses do not violate the terms of use for ChatGPT Enterprise.

- **What rights do you have to own, use, modify, and distribute the lesson plans and other content generated by ChatGPT Enterprise?**

Customer Content. You and End Users may provide input to the Services ("Input"), and receive output from the Services based on the Input ("Output"). We call Input and Output together "Customer Content." As between you and OpenAI, and to the extent permitted by applicable law, you (a) retain all ownership rights in Input and (b) own all Output. We hereby assign to you all our right, title, and interest, if any, in and to Output. ([Business Terms](); 3.1)

You will not, and will not permit End Users to:

(b) use the Services or Customer Content in a manner that infringes, misappropriates, or otherwise violates any third party's rights;

(e) use Output (as defined below) to develop any artificial intelligence models that compete with our products and services. However, you can use Output to (i) develop artificial intelligence models primarily intended to categorize, classify, or organize data (e.g., embeddings or classifiers), as long as such models are not distributed or made commercially available to third parties and (ii) fine tune models provided as part of our Services;

([Business Terms](); 2)

- o Evaluation:

● **What usage limitations has OpenAI placed on using ChatGPT Enterprise and its other tools?**

Restrictions. We own all right, title, and interest in and to the Services. You only receive rights to use the Services as explicitly granted in this Agreement. You will not, and will not permit End Users to:

(a) use the Services or Customer Content (as defined below) in a manner that violates any applicable laws or OpenAI Policies;

(b) use the Services or Customer Content in a manner that infringes, misappropriates, or otherwise violates any third party's rights;

(c) send us any personal information of children under 13 or the applicable age of digital consent or allow minors to use our Services without consent from their parent or guardian;

(d) reverse assemble, reverse compile, decompile, translate, engage in model extraction or stealing attacks, or otherwise attempt to discover the source code or underlying components of the Services, algorithms, and systems of the Services (except to the extent these restrictions are contrary to applicable law);

(e) use Output (as defined below) to develop any artificial intelligence models that compete with our products and services. However, you can use Output to (i) develop artificial intelligence models primarily intended to categorize, classify, or organize data (e.g., embeddings or classifiers), as long as such models are not distributed or made

commercially available to third parties and (ii) fine tune models provided as part of our Services;

(f) use any method to extract data from the Services other than as permitted through the APIs; or

(g) buy, sell, or transfer API keys from, to or with a third party.

([Business Terms](); 2)

Law Compliance: Users must follow applicable laws, respect privacy, avoid regulated activities without proper compliance, and refrain from illegal actions, including child exploitation or illegal substance distribution.

Avoid Harm: Users should not use OpenAI services to harm themselves or others, promote violence, or engage in unauthorized system breaches.

Ethical Use of Outputs: Output from OpenAI services should not be used for fraud, harassment, discrimination, or promoting violence or hatred.

Respect Safeguards: Users should not bypass safety features unless authorized for specific research under OpenAI's Sharing & Publication Policy.

CSAM Reporting: OpenAI reports any apparent child sexual abuse material to relevant authorities.

(https://openai.com/policies/usage-policies/)

- o Evaluation:

4. **Termination.**

Description: Termination rights matter to Learn-a-Lot because they provide essential control over continuity, risk management, and compliance when using OpenAI's services. If OpenAI can terminate the agreement, Learn-a-Lot risks disruptions that could affect its educational programs and incur unexpected costs to find replacement tools. Having clear termination rights allows Learn-a-Lot to plan exit strategies, manage data appropriately, and maintain alignment with its standards, regulatory obligations, and reputational goals.

● **What rights does each party have to terminate the agreement?**

Termination. Unless you purchase Services for a committed duration, you may terminate this Agreement at any time by deleting your account. Both you and OpenAI may terminate this Agreement upon written notice (a) if the other party materially breaches this Agreement and does not cure the breach within thirty (30) days after receiving written notice of the breach or (b) if the other party ceases its business operations or becomes subject to insolvency proceedings. We may suspend your or any End User's access to the Services or terminate this Agreement or any Order Form: (i) if required to do so by law; (ii) to prevent a security risk or other credible risk of harm or liability to us, the Services, or any third party; or (iii) for repeated or material violations of the OpenAI Policies. We will use reasonable efforts to notify you of any suspension or

termination and give you the opportunity to resolve the issue prior to suspension or termination. ([Business Terms](); 8.2)

We have established universal policies applicable to all our services, as well as specific policies for builders who use ChatGPT or our API to create applications for themselves or others. Violating our policies could result in action against your account, up to suspension or termination. We also work to make our models safer and more useful, by training them to refuse harmful instructions and reduce their tendency to produce harmful content. ([Usage Policies]())

  o   Evaluation:

Part II: Additional Considerations for AI Use in Educational Settings

1.   **Limitations of AI in Educational Content Creation**

Scenario: ChatGPT may lack contextual understanding of specific educational standards or nuances, which could lead to generic lesson plans that require additional adaptation by educators.

- **Action**: *Learn-a-Lot!* ensures all content generated with ChatGPT undergoes educator review and aligns with state and local educational standards.

2.   **FERPA Compliance**

Scenario: As an educational nonprofit, *Learn-a-Lot!* must comply with the Family Educational Rights and Privacy Act (FERPA) to protect student information.

- **Evaluation**: OpenAI's terms do not specifically guarantee FERPA compliance. *Learn-a-Lot!* creates and implements a training plan to ensure that all staff members receive training on FERPA standards, particularly when using ChatGPT for lesson planning involving student data.

3.   **State and Local Education Regulations**

Scenario: Certain states and school districts impose rules around AI use in educational settings. *Learn-a-Lot!* needs to ensure ChatGPT usage complies with any relevant local regulations.

- **Action**: *Learn-a-Lot!* consults with local education boards to confirm that using ChatGPT for lesson planning is compliant. They receive preliminary approval and establish a policy for regular compliance reviews, ensuring alignment with any future regulatory changes.

4.   **Audit Preparedness and Data Breach Protocols**

Scenario: *Learn-a-Lot!* must be prepared for audits or potential data breaches, especially if any sensitive information is compromised in connection with ChatGPT usage.

- **Action**: *Learn-a-Lot!* creates an audit preparation and incident response plan. This plan includes logging data access for transparency, conducting regular audits on data security practices, and establishing a clear procedure for notifying stakeholders in the event of a breach.

5. **Transparency to Educators and Administrators**

Scenario: Educators and administrators must understand ChatGPT's role in lesson planning and how it will be used responsibly within *Learn-a-Lot!*'s educational programs.

- **Action**: *Learn-a-Lot!* develops a clear consent policy for educators and administrators, explaining ChatGPT's role in lesson planning. They clarify that ChatGPT is intended to support lesson preparation and creative ideation, not to replace professional expertise, ensuring transparency and understanding among all stakeholders.

Part III: Other Scenarios To Consider

Instructions: Consider these additional scenarios to explore different uses of ChatGPT within *Learn-a-Lot!*'s operations, focusing on potential compliance, privacy, and ethical challenges.

Scenario 1: Internal Use of ChatGPT for Administrative Purposes

- *Description*: *Learn-a-Lot!* may consider using ChatGPT for internal administrative tasks, such as automating communications, creating reports, or generating policy drafts.
- *Considerations*: Review OpenAI's terms regarding data handling and confidentiality for internal use. Ensure data privacy measures align with administrative needs and do not compromise sensitive organizational information.

Scenario 2: Integration of GPT-4o into a Student-Facing Educational Tool

- *Description*: *Learn-a-Lot!* is exploring the possibility of integrating ChatGPT into a learning tool that interacts directly with students, offering on-demand tutoring or answering STEM questions.
- *Considerations*: Review OpenAI's terms for student-facing applications, focusing on compliance with FERPA and state regulations. Establish protocols to monitor interactions and ensure that AI-generated responses are accurate, age-appropriate, and reinforce positive learning.

Scenario 3: Integration of ChatGPT into *Learn-a-Lot!*'s Online Platform for End Users

- *Description*: *Learn-a-Lot!* may embed ChatGPT as part of its online platform, offering resources to educators, parents, and students.
- *Considerations*: Assess OpenAI's terms to understand data ownership and privacy rights when AI is embedded in a publicly accessible platform. Ensure that users' interactions are secure and that platform policies communicate the AI's role clearly, including any limitations or disclaimers.