

Content Transformation Sample

Turning Complex Policy into Clear, Actionable Learning

Project Overview

Challenge

Employees are often required to read lengthy workplace policies containing formal or technical language. While the information may be important, presenting it as a static document can make it difficult for employees to identify what they actually need to know and do.

For this sample, I transformed a fictional workplace information-security policy into concise, learner-focused content suitable for an online learning experience.

ORIGINAL SOURCE CONTENT

Information Security and Confidential Information Policy

Employees are responsible for ensuring that all confidential and sensitive organizational information in their possession or control is appropriately protected against unauthorized access, use, disclosure, modification, loss, or destruction. Employees must exercise reasonable precautions when accessing, transmitting, storing, or disposing of confidential information.

Confidential information should only be accessed by individuals who require such information for legitimate business purposes and who possess the appropriate authorization. Employees must not disclose confidential organizational information to unauthorized individuals, whether internally or externally.

Employees who become aware of an actual or suspected loss, unauthorized disclosure, security breach, or inappropriate access involving confidential information are required to immediately report the incident to their supervisor and the appropriate information security personnel in accordance with organizational procedures.

Failure to comply with information security policies and procedures may result in corrective or disciplinary action.

TRANSFORMED LEARNING CONTENT

Protecting Confidential Information

Every day, you may work with information that shouldn't be seen by everyone.

Protecting that information is part of your responsibility.

Before accessing or sharing confidential information, ask yourself:

Do I need this information to do my job?

Only access confidential information when you have a legitimate work-related reason and the appropriate authorization.

Is the person I'm sharing it with authorized to receive it?

Before sending or discussing confidential information, make sure the recipient is authorized to access it.

Am I handling the information securely?

Take appropriate precautions when viewing, storing, sending, or disposing of confidential information.

What Would You Do?

You accidentally send a document containing confidential information to the wrong person.

What should you do?

- A.** Ask the recipient to delete the message and continue working.
- B.** Wait to see if the recipient opens the document.
- C.** Report the incident immediately using your organization's security reporting process.

Correct Answer: C

Report suspected or confirmed security incidents as soon as possible.

Reporting an incident quickly allows the appropriate team to assess the situation and take action to reduce potential harm.

Even if the disclosure was accidental, it should still be reported.

Remember

When working with confidential information:

- Access only what you need.
- Share information only with authorized people.
- Handle and store information securely.
- Report suspected security incidents immediately.

When in doubt, check your organization's information-security procedures or ask the appropriate person before sharing sensitive information.

DESIGN RATIONALE

The original policy communicates important requirements but relies on formal language and long sentences. Simply placing the policy into an online course would transfer the information without necessarily helping learners understand how to apply it.

The revised version reorganizes the content around decisions an employee may need to make at work.

The transformation uses:

Plain language — Formal policy language is replaced with shorter, more conversational explanations while preserving the intent of the source material.

Action-oriented content — Learners are given four clear behaviours: access appropriately, share carefully, protect information, and report incidents.

Chunking — Information is divided into smaller sections to reduce cognitive load.

Decision-based learning — A workplace scenario asks learners to apply the information rather than simply recall policy language.

Immediate feedback — The learner receives an explanation of the correct action and why it matters.

The objective is not to replace the organization's official policy. The learning experience helps employees understand the behaviours expected of them while allowing the original policy to remain the authoritative source.