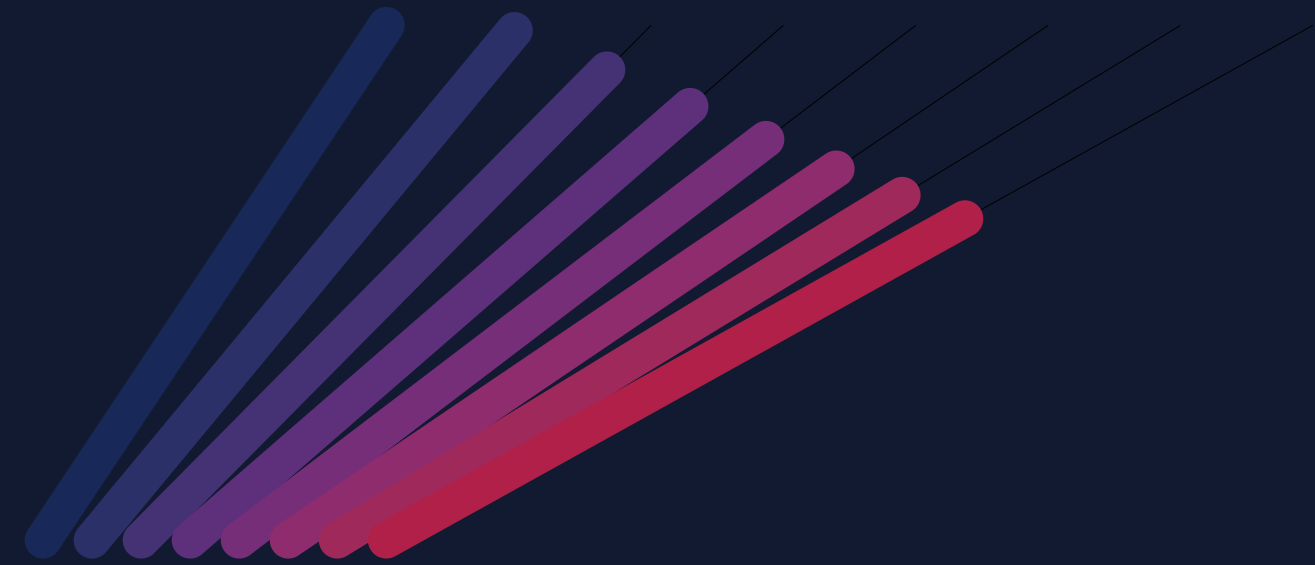




AX 디자인팩토리 부트캠프

청년도약 인재양성 부트캠프 · 온라인 과정

무엇을 넣으면 안 되 나 — 개인정보와 기밀

1강 · 무엇을 넣으면 안 되나 — 개인정보와 기밀

과목
AI 활용 윤리와 가이드라인

차시
1 / 4

길이
27분

도입

오늘 정하는 것

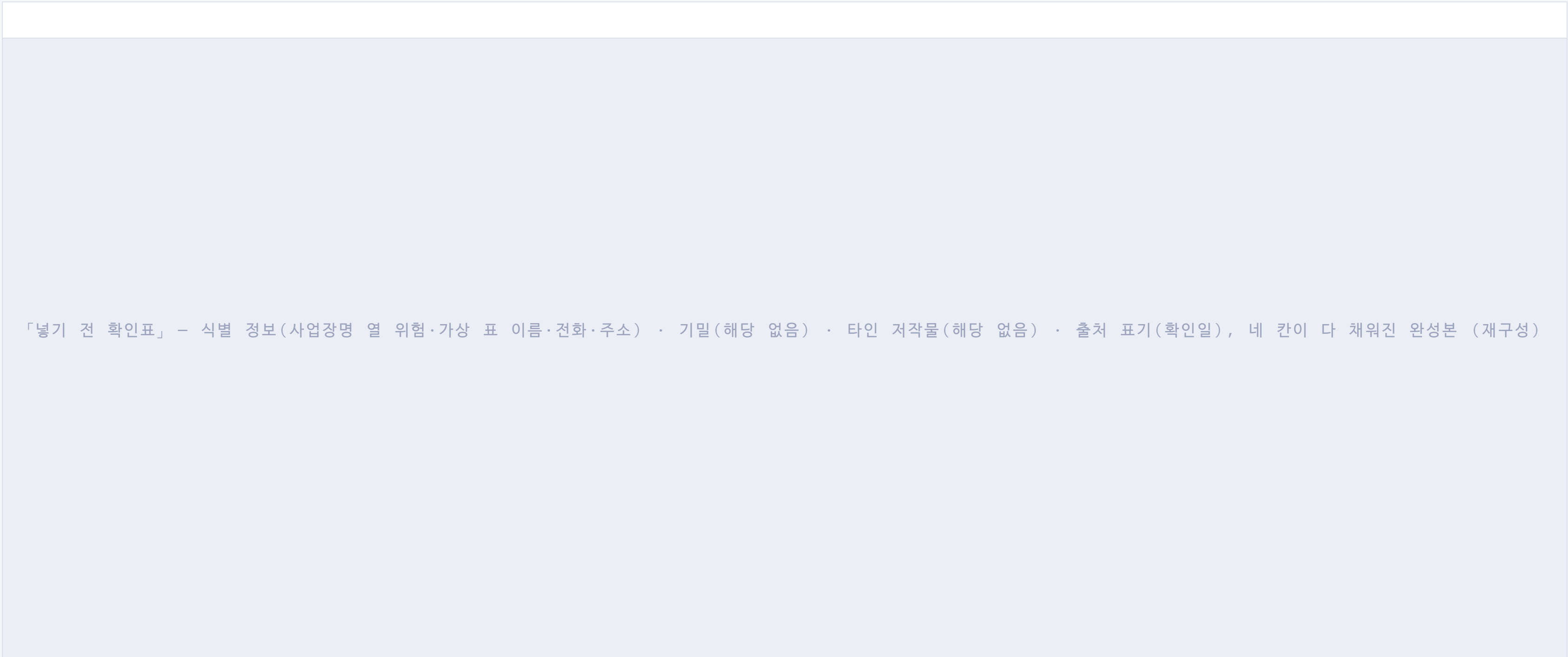
이 편이 끝나면 한 문장에 답할 수 있어야 합니다.

Q AI에게 넣기 전에 무엇을 확인해야 하는가

답을 못 하면 열 이름만 보고 그대로 넣게 됩니다.

도입

이 편이 끝나면 보는 것



「넣기 전 확인표」 - 식별 정보(사업장명 열 위험·가상 표 이름·전화·주소) · 기밀(해당 없음) · 타인 저작물(해당 없음) · 출처 표기(확인일), 네 칸이 다 채워진 완성본 (재구성)

이 편 시연 설계(확인표 네 칸) - 집필자 구성 · 확인일 2026-09-06

도입 · 과목이 남기는 것

책임이 갈리는 세 지점

- 1 넣은 것 — AI에게 건네는 자료(오늘)
- 2 나온 것 — AI가 만들어 낸 결과물(다음 차시)
- 3 내보낸 것 — 결과물을 공유하거나 제출하는 행위(그 뒤)

이 과목에서만 다루는 것

도구

Antigravity, 프리뷰 무료

- 구글 계정으로 로그인
- 오픈코드·커서 CLI 등으로 바뀌도 됨

막히면

대처 경로 셋

- 나눠서
- 다른 도구로
- 텍스트로

입력의 경계

이론

6분

소재 없이 — 넣기 전에 셋을 본다

넣기 전에 확인할 것은 셋이다.

식별 가능한 개인정보 · 조직의 기밀 · 타인의 저작물

열 이름이 아니라 실제 값이 기준입니다.

이론 · 다른 예

기밀 쪽 극단과 개인정보 쪽 극단

삼성전자 사고

소스코드·회의 내용을 그대로 입력

- 회사가 사내 기기에서 생성형 AI 사용을 금지
- 되돌릴 방법이 없었다

의료 · 법률 상담

사정 자체가 특정 정보

- 이름을 지워도 서술만으로 짐작 가능
- 서술 전체가 경계 대상

지우는 것보다 넣지 않는 것

- 1 일부 서비스 약관은 입력 내용을 학습에 다시 쓸 수 있다고 정한다
- 2 한 번 넣은 문장은 어딘가에 남을 가능성을 배제할 수 없다
- 3 서비스마다 조항이 다르니 확인이 안 되면 넣지 않는 쪽을 기본값으로 둔다

두 파일을 열어 본다

시연

13분

이름표가 아니라 실제 값을 본다

「주관식」 라벨의 정체 (재구성)



설문 파일 (31,635행 × 22열)을 AI에 넣어 분류시키려다 먼저 열어 본다 — 우리 보고서가 "주관식"이라 적었지만 화면에 뜨는 실제 열 이름은 「지역경제활성화를 위한 노력」, 자유 텍스트가 아니라 고유값 35개 선택형에 최빈값은 무응답 코드 999

`assets/data/daejeon/README.md` 더러운 원천 실측 · 원자료 author-c/probe-dj/3b/data/survey.csv · 확인일 2026-09-06

「사업장명」 열은 화면에 올리지 않는다 (사실만 말로 · 가상 재구성)

인허가업소 파일에 「사업장명」 열이 있어 개인 이름이 섞일 수 있다는 사실만 말로 확인 (실제 값은 열지 않는다) - 대신 이름·전화·주소를 가상 값으로 채운 재구성 표 (실존 인물 아님)로 「넣기 전 확인표」를 채운다

시연 · 함정

AI에게 “지워 줘” 시킨 결과 (재구성·가상)

항목	AI가 지움	사람이 다시 검사
전화	지움	확인 완료
이름	남음	사람이 마스킹 추가

이 편 시연 설계(가상 표 대조, 실존 인물 아님) · 확인일 2026-09-06

열기 전에 알 수 없다

정리

넣기 전에 열어 봅니다. 열어 보면 넣을 필요가 없을 때가 많습니다.

다음 차시

나온 것은 누구 것인가 — 저작권과 학습 데이터

배웠는지 재는 질문 — 이 파일에서 AI에게 넣으면 안 되는 열은 무엇입니까?

