
MANUALE OPERATIVO

Integrazione Gemini API nel Sistema AT Scuole

Destinatari	Personale ATA, amministratori di sistema scolastico
Contesto	Amministrazione Trasparente – DM 219
AI integrata	Google Gemini API (via proxy sicuro)
Versione	1.0 — Maggio 2025

Indice

- Indice 2
- 1. Obiettivo 3
- 2. Regola Fondamentale di Sicurezza 4
- 3. Architettura Consigliata 5
 - Come funziona il proxy 5
- 4. Passaggi Operativi 6
 - 4.1 Caricamento file sul server 6
 - 4.2 Configurazione chiave API 6
 - 4.3 Configurazione e test..... 6
- 5. Prompt Istituzionale Consigliato..... 7
 - Elementi chiave del prompt 7
- 6. Privacy e Cautele 8
- 7. Aggiornamento della Knowledge Base 9
 - Procedura di aggiornamento 9
- 8. Modalità Senza Gemini 10
- 9. Nota Didattica — DM 219 11

1. Obiettivo

Questo manuale spiega come collegare il sito "Manuale operativo Amministrazione Trasparente per le scuole" a un'intelligenza artificiale di proprietà o sotto controllo della scuola, ipotizzando l'uso delle API Google Gemini.

Il principio tecnico di base è semplice: l'AI risponde esclusivamente usando la knowledge base knowledge.md, che resta modificabile e aggiornabile dalla scuola in modo autonomo.

Vantaggio principale

La scuola mantiene il controllo completo dei contenuti. L'AI non inventa informazioni: legge solo ciò che il personale scolastico ha inserito nel file knowledge.md.

2. Regola Fondamentale di Sicurezza

⚠ Regola critica — da non violare mai

Non inserire mai la chiave API Gemini all'interno del file index.html o in qualsiasi altro file JavaScript pubblico. Chiunque acceda al sito potrebbe leggere la chiave e utilizzarla a spese dell'istituto.

La chiave API deve risiedere esclusivamente lato server, attraverso uno dei seguenti metodi:

Metodo	Descrizione
Variabile d'ambiente	GEMINI_API_KEY definita nel pannello di controllo del server (cPanel, .env, ecc.)
File di configurazione	File PHP o JSON non pubblico, fuori dalla webroot
Secret Manager cloud	Google Secret Manager, AWS Secrets Manager o equivalente
Proxy server	Apps Script, Cloud Run, server PHP protetto – vedi Sez. 3

3. Architettura Consigliata

Il flusso corretto prevede che il browser dell'utente non comunichi mai direttamente con le API Google. Ogni richiesta transita dal proxy server della scuola, che gestisce la chiave in modo sicuro.

```
Utente → Sito web → /api/gemini-proxy.php → Gemini API → Risposta
```

Come funziona il proxy

- Il sito invia al proxy solo la domanda dell'utente (nessun dato sensibile)
- Il proxy legge il file knowledge.md sul server
- Seleziona i blocchi pertinenti alla domanda ricevuta
- Costruisce il prompt completo (istruzioni + knowledge + domanda)
- Chiama Gemini API con la chiave segreta
- Restituisce la risposta al sito, senza esporre la chiave

Beneficio di questa architettura

Il file knowledge.md e la chiave API non vengono mai inviati al browser. L'utente riceve solo la risposta elaborata da Gemini, filtrata dal prompt istituzionale.

4. Passaggi Operativi

4.1 Caricamento file sul server

Caricare sul server le seguenti risorse tramite FTP/SFTP o cPanel File Manager:

File / Cartella	Contenuto
index.html	Interfaccia web del sito AT Scuole
knowledge.md	Knowledge base aggiornabile dalla scuola
assets/	Immagini, CSS, JavaScript del sito
api/	Cartella contenente gemini-proxy.php

4.2 Configurazione chiave API

1. Accedere a Google AI Studio (aistudio.google.com) o alla console Google Cloud/Workspace dell'ente.
2. Generare una nuova chiave API Gemini con le autorizzazioni necessarie.
3. Salvare la chiave come variabile d'ambiente denominata GEMINI_API_KEY nel pannello di controllo del server.
4. Verificare che il file `api/gemini-proxy.php` non esponga la chiave nel codice sorgente pubblico.

4.3 Configurazione e test

5. Aprire il sito dal browser e accedere alle impostazioni dell'endpoint.
6. Impostare come endpoint: `/api/gemini-proxy.php`
7. Fare una domanda di prova: "Chi è il responsabile della pubblicazione in Amministrazione Trasparente?"
8. Verificare che la risposta indichi: Dirigente scolastico, fonte interna da `knowledge.md`, eventuale necessità di verifica normativa.

Test di validazione riuscito

Se la risposta menziona il Dirigente scolastico come responsabile e cita la knowledge interna senza inventare norme o scadenze, il sistema è configurato correttamente.

5. Prompt Istituzionale Consigliato

Il proxy server utilizza un prompt strutturato che viene anteposto a ogni richiesta inviata a Gemini. Questo prompt definisce il comportamento dell'AI e garantisce risposte pertinenti e sicure.

```
Rispondi come assistente operativo per una scuola italiana.  
Usa esclusivamente la knowledge fornita.  
Se l'informazione non è presente o è incerta,  
dichiara che serve verifica su fonte ufficiale.  
Non inventare norme, scadenze o responsabilità.  
Ricorda che il responsabile della pubblicazione  
in Amministrazione Trasparente è il Dirigente scolastico.
```

Elementi chiave del prompt

Elemento	Scopo
Ruolo istituzionale	Limita l'AI al contesto scolastico italiano
Uso esclusivo della knowledge	Impedisce allucinazioni e invenzioni normative
Dichiarazione di incertezza	Evita risposte false con tono di certezza
Responsabile pubblicazione	Ancora un'informazione istituzionale critica e non modificabile

6. Privacy e Cautele



Dati da non inviare mai a Gemini

Il sistema non è omologato per il trattamento di categorie particolari di dati personali. Rispettare scrupolosamente i seguenti divieti per garantire la conformità al GDPR.

Categoria vietata	Motivazione
Dati sanitari	Dati sensibili ex art. 9 GDPR
Dati di minori	Tutela rafforzata per soggetti vulnerabili
Dati giudiziari	Dati sensibili ex art. 10 GDPR
Graduatorie con CF o dati L. 104/1992	Rischio di profilazione illecita
Documenti interni non anonimizzati	Dati non necessari alla finalità del sistema
Segnalazioni disciplinari	Dati riservati e non pertinenti

Per simulazioni o test, utilizzare sempre esempi completamente anonimi e privi di riferimenti reali a persone fisiche.

7. Aggiornamento della Knowledge Base

La knowledge base è il cuore del sistema. Tenerla aggiornata garantisce risposte accurate e conformi alle ultime disposizioni normative.

Procedura di aggiornamento

9. Aprire il file knowledge.md con un editor di testo (es. VS Code, Notepad++, TextEdit).
10. Modificare o aggiungere le informazioni necessarie (nuova norma, correzione di errore, aggiornamento scadenza).
11. Salvare il file con codifica UTF-8.
12. Ricaricare il file sul server tramite FTP/SFTP, sostituendo la versione precedente.
13. Aprire il sito e ripetere una domanda di test correlata alla modifica.
14. Verificare che la risposta rifletta correttamente l'aggiornamento.

Attenzione alle versioni divergenti

Il sito e Gemini devono leggere sempre la stessa versione di knowledge.md. Non mantenere copie separate del file in cartelle diverse: una sola fonte di verità, un solo file sul server.

8. Modalità Senza Gemini

Il sistema è progettato per funzionare anche in assenza di connessione alle API Gemini. In questa modalità, il sito effettua una ricerca locale sul file knowledge.md e restituisce le voci più pertinenti alla domanda. IL SISTEMA FUNZIONA IN LOCALE SU UN SEMPLICE PC SEMPLICEMENTE CLICCANDO SU INDEX.HTML. E' PROBABILE CHE IN BASSO IL SISTEMA VI CHIEDA DI INVIARE LA KNOWLEDGE, IN TAL CASO INSERITE QUELLA FORNITA O QUELLA CHE AVETE MODIFICATO DIRETTAMENTE.

Aspetto	Con Gemini API	Senza Gemini API
Qualità risposta	Discorsiva, contestuale	Voci pertinenti elencate
Dati inviati all'esterno	Domanda (anonima) a Google	Nessuno
Requisiti server	PHP + chiave API + internet	Solo file statico
Complessità setup	Media	Minima

La modalità senza Gemini è consigliata per scuole che non possono o non vogliono inviare dati a servizi esterni, o come soluzione di riserva in caso di indisponibilità delle API.

9. Nota Didattica — DM 219

Questo sistema può essere presentato e utilizzato come esempio concreto di laboratorio formativo per personale ATA e per le scuole che vogliono avvicinarsi all'uso responsabile dell'intelligenza artificiale in ambito amministrativo.

1	Partire da un bisogno amministrativo reale (Amministrazione Trasparente)
2	Costruire una knowledge base controllabile e aggiornabile dal personale scolastico
3	Generare un sito consultabile, accessibile e senza barriere tecnologiche
4	Integrare un'AI controllata con prompt trasparente e revisionabile
5	Mantenere sempre la revisione umana come ultimo livello di controllo

Principio guida

L'AI è uno strumento al servizio del personale scolastico, non un sostituto. La responsabilità delle informazioni pubblicati in Amministrazione Trasparente rimane sempre in capo al Dirigente scolastico e al personale incaricato.