DIRITTO E TECNOLOGIA

Intelligenza Artificiale: Quadro Normativo

Relatrice: **Dott.ssa Maria Riccardo** – *Consulente ed Esperta Privacy*

Moderatrice: ***Rossella Gobbo -***



QUADRO NORMATIVO

Interventi normativi europei e

GDPR — Reg. UE 679/2016

Disciplina generale sulla protezione dei dati personali nell'UE. Costituisce la base fondamentale per la regolamentazione dell'intelligenza artificiale in Europa.

AI Act — Reg. UE 1689/2024

Primo quadro normativo organico sullo sviluppo e utilizzo dell'IA nel mercato europeo. Introduce un approccio basato sul rischio.

DDL n°78/2024

Proposta normativa nazionale del Consiglio dei Ministri per l'implementazione italiana delle regole europee sull'intelligenza artificiale.

Linee Guida MIM 166/2025

Direttive ministeriali per l'utilizzo dell'IA nel contesto educativo e formativo italiano.

Legge 132/2025

Normativa nazionale definitiva sui principi e l'applicazione dell'IA in Italia. In vigore dal **10 ottobre 2025**.

Norma UNI 11621-8 30 Aprile 2026

definisce i profili di ruolo professionale operanti nel settore dell'Intelligenza Artificiale

NORMATIVA DI RIFERIMENTO

L'intelligenza artificiale deve essere conforme al GDPR

Il GDPR rappresenta la **prima e principale normativa di riferimento** per qualsiasi sistema di IA che tratti dati personali. Il Garante della privacy italiano ha già adottato provvedimenti restrittivi nei confronti di piattaforme quali **ChatGPT** — temporaneamente vietato per assenza di base giuridica e informativa adeguata — e **DeepSeek**, bloccato per analoghe carenze di conformità. Tali interventi evidenziano la necessità di un approccio rigoroso nella gestione dei dati personali da parte dei sistemi di IA.



IA E GDPR

Dati personali e intelligenza artificiale

I sistemi di IA sono **interattivi, autonomi e adattabili**. Il **machine learning** — nelle sue forme evolute di deep learning e reinforcement learning — consente agli algoritmi di modificarsi autonomamente *ex post*, aprendo questioni cruciali di responsabilità civile e penale.

L'IA necessita di dati personali per funzionare. Con la diffusione dell'IA generativa e dei sistemi consumer, gli utenti cedono quantità crescenti di dati spesso **senza piena consapevolezza** delle conseguenze.

Identificazione diretta

Dati anagrafici, immagini, dati biometrici

Identificazione indiretta

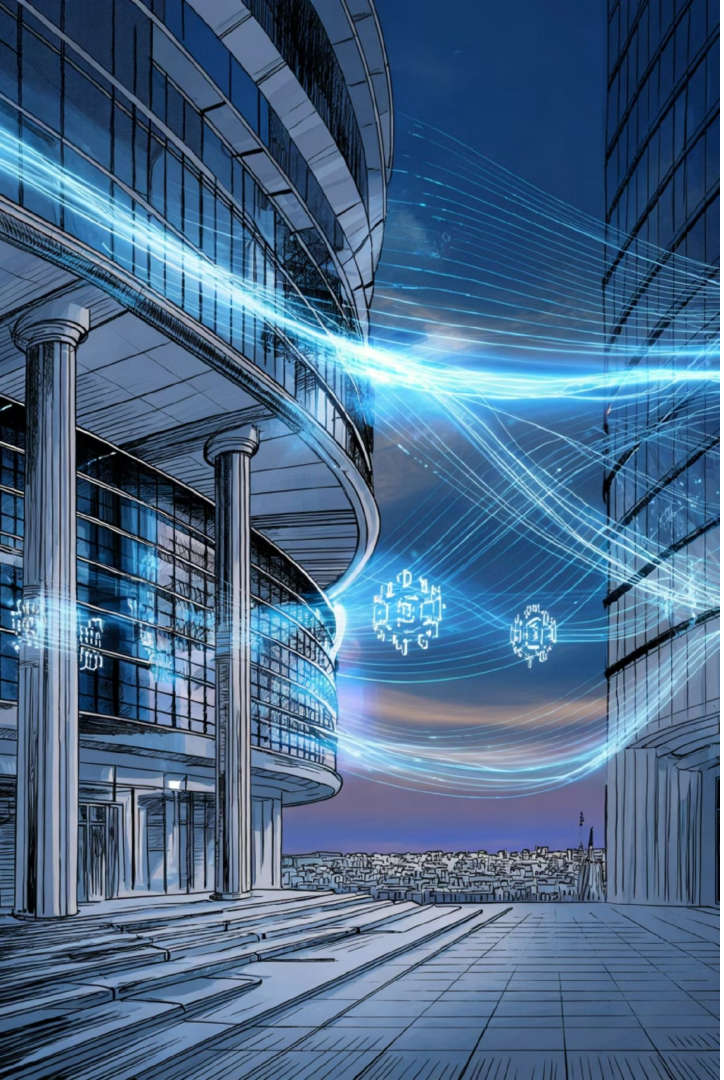
Codice fiscale, indirizzo IP, targa, IBAN

Categorie particolari

Origine etnica, salute, opinioni politiche, dati genetici

Dati giudiziari

Condanne penali, misure di sicurezza, qualità di imputato



I Act — Reg. UE 1689/2024

Un approccio normativo basato sul rischio

1

🚫 Rischio inaccettabile

Sistemi vietati: scoring sociale, manipolazione subliminale

2

⚠️ Alto rischio

Requisiti rigorosi: infrastrutture critiche, istruzione, occupazione

3

ℹ️ Rischio limitato

Soggetti a obblighi di trasparenza: I soggetti devono sapere di interagire con strumenti Ai (es.Chatbot, deepfake.)

4

✅ Rischio minimo

Quando l'Ai svolge un ruolo di suggeritore e non di decisore

Questa classificazione si integra con il GDPR, creando un ecosistema normativo più completo per la gestione dei sistemi di IA e dei dati personali che utilizzano.

AI ACT — ART. 5

Pratiche vietate: manipolazione e social scoring

Manipolazione e sfruttamento delle vulnerabilità

Vietati i sistemi che utilizzano tecniche subliminali o sfruttano vulnerabilità legate a **età, disabilità o condizione socioeconomica** per distorcere il comportamento causando danni fisici o psicologici. Il divieto si applica quando tutte e quattro le condizioni sono soddisfatte simultaneamente.

⚠ Esempi: algoritmi che propongono prodotti finanziari rischiosi ad anziani sfruttandone le limitazioni cognitive.

Social scoring — pubblico e privato

Il **punteggio sociale** è vietato sia per autorità pubbliche che per soggetti privati. I rischi principali includono:

- Esclusione da servizi pubblici essenziali
- Discriminazione sistematica basata su attività politiche o sociali
- Sorveglianza massiva del comportamento online
- Classificazione discriminatoria di clienti e lavoratori da parte di aziende private

AI ACT — DIVIETI

Pratiche vietate: biometria, emozioni e

Identificazione biometrica remota in tempo reale

Vietata negli spazi pubblici per finalità di contrasto, salvo eccezioni strettamente regolamentate. Vietata anche la categorizzazione biometrica basata su caratteristiche sensibili: etnia, religione, orientamento sessuale, opinioni politiche.

Riconoscimento delle emozioni sul lavoro e a scuola

Vietato, salvo finalità mediche o di ricerca. Il significativo **squilibrio di potere** nel contesto lavorativo rende questi strumenti altamente invasivi: monitoraggio dell'attenzione, rilevamento dello stress, analisi delle espressioni facciali.

Sistemi predittivi di polizia per profilazione

Vietata la valutazione del rischio di reato basata esclusivamente su caratteristiche personali (etnia, luogo di nascita, status socioeconomico). Generano pregiudizi, discriminazioni e **ingiustizie algoritmiche**.

Database di riconoscimento facciale da scraping

Vietata la raccolta indiscriminata di immagini da internet o videosorveglianza. Viola il GDPR, il principio di limitazione delle finalità e abilita la sorveglianza di massa senza consenso degli interessati.

Rispetto della privacy nell'uso pratico dell'IA

Evitare dati particolari nelle richieste

Non inserire informazioni personali particolari nelle richieste ai sistemi di IA. Ogni dato condiviso potrebbe essere utilizzato per l'addestramento degli algoritmi o conservato sui server dell’applicativo.

Protezione dei dati degli studenti

In ambito educativo, è fondamentale non richiedere all'IA di elaborare dati personali degli studenti: nomi completi, risultati scolastici, valutazioni individuali o altre informazioni identificative.

Consapevolezza delle implicazioni legali

Il GDPR impone restrizioni rigorose. Ogni utilizzo di sistemi di IA che trattano dati personali deve essere preceduto da una valutazione delle implicazioni legali e da una verifica di conformità normativa.

Formazione e sensibilizzazione continua

La formazione degli utenti è elemento cruciale per garantire un utilizzo consapevole e conforme dell'IA, in linea con le normative vigenti sulla protezione dei dati personali.

NORMATIVA ITALIANA

Il quadro normativo nazionale

Il legislatore italiano integra e specifica l'applicazione delle disposizioni europee sul territorio nazionale, definendo principi, competenze e modalità operative per un utilizzo responsabile dell'intelligenza artificiale.

Recepimento direttive europee

Trasposizione dell'AI Act e del GDPR nell'ordinamento italiano

Adattamento al contesto nazionale

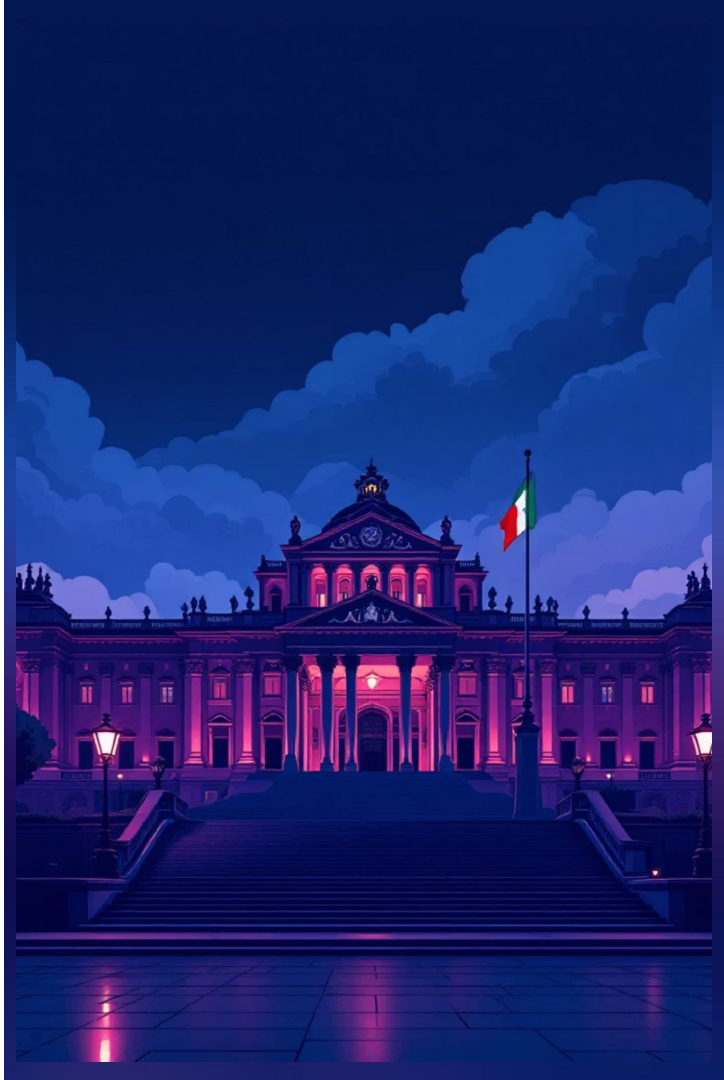
Specificità italiane nella regolamentazione e nelle procedure

Definizione autorità competenti

Ruolo del Garante Privacy e delle autorità di vigilanza settoriali

Modalità di implementazione

Legge 132/2025 in vigore dal 10 ottobre 2025



Principi guida per un'IA conforme e responsabile

Legalità e base giuridica

Ogni trattamento di dati personali tramite sistemi di IA richiede una base giuridica valida ai sensi del GDPR e conformità all'AI Act.

Proporzionalità e minimizzazione

I dati devono essere strettamente necessari alla finalità perseguita, evitando trattamenti eccessivi o sproporzionati.

Trasparenza e responsabilità

Deployer di sistemi di IA sono tenuti a garantire trasparenza verso gli interessati e a dimostrare conformità normativa continuativa.



NORMATIVA IA

Come Utilizzare l'IA Secondo la Normativa

Una guida essenziale per comprendere i principi fondamentali e gli obblighi normativi nell'utilizzo dell'intelligenza artificiale in Italia, con focus su trasparenza, protezione dati e supervisione umana.





Approccio Antropocentrico e Supervisione Umana

L'IA deve essere impiegata come **strumento di supporto**, con intervento umano costante e responsabilità esplicita sulle decisioni sensibili: *"al servizio della persona, nel rispetto della dignità, della libertà e dei diritti fondamentali"*.

Il Parallelismo con il GDPR

Come l'art. 22 del GDPR riconosce il diritto a non essere sottoposto a decisioni interamente automatizzate, anche l'IA richiede valutazioni complesse per garantire la centralità umana.

Requisiti Operativi Essenziali

- Audit umani regolari sui processi decisionali
- Tracciabilità completa delle decisioni automatizzate
- Sistema strutturato di supervisione continua
- Formazione specialistica dei progettisti e operatori

Trasparenza nei Confronti degli Utenti

Le imprese e gli enti che utilizzano strumenti di IA devono informare gli utenti in modo **chiaro e preciso** sulle modalità di utilizzo. Nelle attività intellettuali professionali, l'uso di sistemi AI deve essere comunicato esplicitamente, con attenzione ai requisiti di consenso per età.

Sotto i 13 anni

Divieto assoluto di utilizzo di strumenti di IA

13–14 anni

Il consenso deve essere richiesto ai **genitori o tutori legali** prima di qualsiasi utilizzo.

14 anni e oltre

Il consenso è richiesto **direttamente all'utente**, che acquisisce piena capacità decisionale.

Riferimento normativo: L. 132/2025, Art. 4 — Requisiti di consenso specifici per fascia d'età.

La Oxfirm srl suggerisce che il consenso deve essere richiesto ai genitori o tutori legali, per i minori di 18 anni.

LINEE GUIDA WP29 — DICEMBRE 2016 & APRILE 2017

DPO: Le Responsabilità e i Limiti di Imputazione

Principio fondamentale: In caso di trattamenti **NON conformi** al Regolamento europeo, il DPO **non è personalmente e direttamente responsabile**. Gli obblighi di conformità gravano esclusivamente sul **titolare** e sul **responsabile del trattamento**, secondo quanto chiarito dalle Linee Guida del Gruppo dei Garanti Europei ex art. 29.

Il DPO può tuttavia incorrere in specifiche forme di responsabilità in relazione alla propria posizione giuridica e al contesto in cui opera. La distinzione tra le fattispecie è essenziale per una corretta gestione dei rischi legali connessi alla figura.

Responsabilità Contrattuale

Si configura quando il DPO è **esterno** all'organizzazione: in caso di inadempimento degli obblighi previsti dal contratto di incarico, il DPO può essere chiamato a rispondere nei confronti del titolare per i danni derivanti dall'inadempimento.

Responsabilità Amministrativa

Riguarda il DPO che opera negli **enti pubblici**: può essere soggetto ad azione di **rivalsa** da parte dell'ente nei casi in cui il danno erariale sia imputabile a **dolo o colpa grave** del DPO stesso.



Chi è responsabile?

La responsabilità primaria per la conformità al GDPR rimane sempre in capo al **Titolare** e al **Responsabile del trattamento**. Il DPO è un organo di controllo e consulenza, non di imputazione diretta.

Governance e Ambiti Applicativi Strategici

Settori ad Alta Vigilanza

Pubblica Amministrazione

Massima trasparenza e accountability verso i cittadini.

Lavoro

Tutela dei diritti dei lavoratori nei processi di selezione e valutazione.

Sanità

Supervisione medica obbligatoria nei sistemi diagnostici e terapeutici.

Settore Giudiziario

Garanzie procedurali rafforzate nell'impiego dell'IA in ambito legale.



Le Autorità Nazionali Competenti

ACN — Vigilanza, ispezioni e sanzioni sui sistemi IA.

AgID — Promozione, notifiche e casi d'uso sicuri.

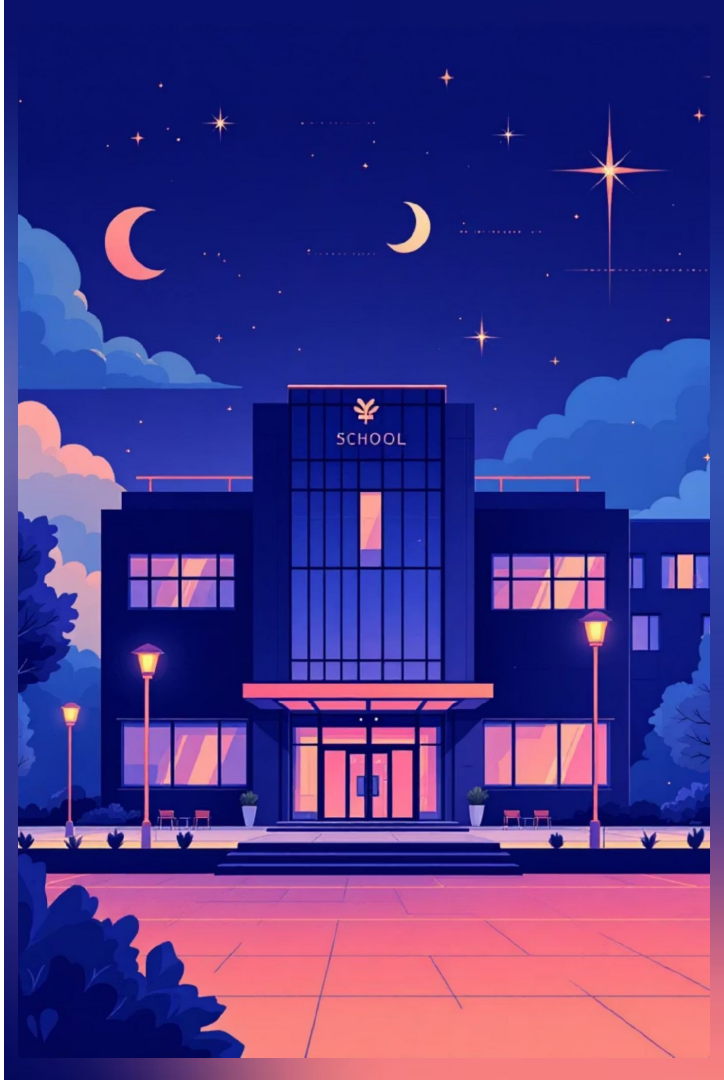
La Strategia nazionale per l'IA è aggiornata ogni due anni con monitoraggio annuale al Parlamento.

INNOVAZIONE DIGITALE

ISTRUZIONE

Linee Guida Ministeriali sull'Intelligenza Artificiale nelle Scuole

Allegato al **Decreto Ministeriale n. 166 del 9 agosto 2025** — un quadro normativo per l'integrazione responsabile dell'IA nel sistema scolastico italiano.



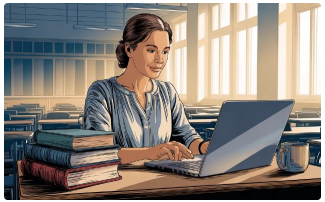
I Tre Ambiti di Applicazione dell'IA

L'intelligenza artificiale rappresenta una risorsa strategica per trasformare l'esperienza educativa e ottimizzare i processi delle istituzioni scolastiche italiane.



Didattica per gli Studenti

Strumenti innovativi che personalizzano l'apprendimento attraverso esperienze educative su misura per ogni alunno.



Supporto ai Docenti

Risorse digitali che assistono gli insegnanti nella progettazione didattica, valutazione e gestione delle attività formative.



Dirigenza e Organizzazione Scolastica

Soluzioni per supportare i DS e velocizzare l'attività degli amministrativi, ottimizzando l'efficienza della segreteria.

Benefici dell'IA per l'Apprendimento degli Studenti



Stimolo alla Curiosità

Esperienze educative coinvolgenti che trasformano lo studio in una scoperta continua.



Risorse Multidisciplinari

Materiali integrati provenienti da diverse discipline per una visione olistica del sapere.



Feedback Immediati

Valutazioni istantanee per correggere errori e consolidare le competenze acquisite.



Accessibilità e Inclusione

Strumenti che abbattono barriere e valorizzano le diversità, rendendo l'istruzione accessibile a tutti.



Autonomia nell'Apprendimento

Percorsi personalizzati che sviluppano competenze di autogestione e indipendenza.



Approfondimento in Tempo Reale

Accesso immediato a spiegazioni supplementari e chiarimenti personalizzati durante lo studio.

L'IA al Servizio dei Docenti



Opportunità per i Docenti

L'intelligenza artificiale offre strumenti avanzati che rivoluzionano l'approccio didattico, consentendo agli insegnanti di dedicare più tempo alla relazione educativa.

- **Personalizzazione dei materiali didattici** adattati agli stili di apprendimento individuali
- **Strumenti interattivi e innovativi** per lezioni più coinvolgenti ed efficaci
- **Supporto nel tutoraggio** degli studenti con bisogni specifici
- **Diversificazione dell'offerta formativa** con percorsi su misura per interessi ed esigenze

IA al servizio dei Dirigenti e Personale

Per il Dirigente Scolastico

- Monitoraggio automatizzato dei documenti programmatici e della loro conformità normativa
- Supporto strategico nella pianificazione delle attività di formazione del personale
- Ottimizzazione intelligente nella riorganizzazione dell'orario scolastico
- Miglioramento della qualità e tempestività della comunicazione istituzionale

Per il Personale Amministrativo

- Organizzazione efficiente e prioritizzazione delle richieste e pratiche amministrative
- Gestione automatizzata di comunicazioni periodiche e circolari
- Sistema intelligente per la gestione dell'inventario dei beni mobili della scuola



Google Docs: La Fine del Foglio Bianco

Scenario Card: Scenario: Avvio corsi pomeridiani di recupero (Matematica e Inglese).

Il Ponte della Trasformazione



Il Passato:
Foglio Bianco

Scrivi una circolare scolastica formale rivolta ai genitori e ai docenti per annunciare l'inizio dei corsi di recupero...

Includi uno spazio per le date e specifica che la frequenza è obbligatoria per gli studenti segnalati.

Il Presente:
L'IA come Collaboratore



Il Futuro:
Documento Pronto

Magia dell'IA - Funzione Riscrivi
Prendi una circolare burocratica e chiedi: "Rendi questo testo più semplice e chiaro per le famiglie non italofone".

NotebookLM

1

Docs - Sciopero

Crea la bozza formale di una comunicazione per annunciare uno sciopero del personale.

2

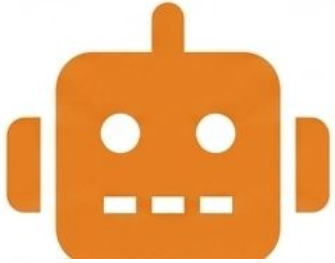
Sheets - Adesioni

Genera una tabella per raccogliere le adesioni allo sciopero (Nome, Ruolo, Adesione Sì/No).

3

Gmail - Chiusura

Scrivi una risposta automatica cortese da impostare per i periodi di chiusura estiva o festiva.



NotebookLM

MINISTERO DELL'ISTRUZIONE DELL'UNIVERSITA' E DELLA RICERCA

STRUTTURA NORMATIVA

I Quattro Pilastri delle Linee Guida

Il Framework ministeriale si articola su quattro componenti fondamentali che garantiscono un'implementazione efficace e responsabile dell'intelligenza artificiale nel contesto educativo italiano.

I Principi

Valori etici fondamentali che guidano ogni scelta nell'adozione dell'IA

Requisiti di Base

Standard tecnici, etici e normativi da rispettare obbligatoriamente

Framework di Implementazione

Metodologia strutturata per introdurre l'IA nelle scuole

Comunicazione e Governance

Strategie per gestire e monitorare l'adozione tecnologica



Principi Fondamentali per l'Uso dell'IA

Centralità della Persona

Il focus è sempre rivolto alla persona e al suo sviluppo integrale. L'IA è al servizio dell'essere umano, mai il contrario.

Equità e Pari Opportunità

Promuovere pari accesso ai benefici della tecnologia, indipendentemente da caratteristiche individuali o contesti di provenienza.

Innovazione Etica e Responsabile

L'IA promuove apprendimento critico e creativo, valorizzando autonomia e impegno individuale senza sostituire la persona.

Sicurezza dei Sistemi

Misure organizzative e tecniche garantiscono alti standard di sicurezza, prevenendo ogni utilizzo improprio delle informazioni.

Tutela dei Diritti Fondamentali

Rispetto dei diritti fondamentali con particolare attenzione a protezione dei dati, riservatezza e non discriminazione.

Requisiti di Base: Aspetti Etici e

Requisiti Etici

Sorveglianza Umana

Monitoraggio continuo per identificare precocemente anomalie nei sistemi di IA.

Trasparenza e Spiegabilità

Tutti devono comprendere chiaramente come funzionano i sistemi implementati.

Diritto di Non Partecipazione

Gli interessati possono decidere se alimentare con i propri dati i sistemi di IA.

Equità del Sistema

Garanzia di uguali opportunità di accesso e beneficio per tutti.

Requisiti Tecnici

Certificazioni dei Produttori

La selezione deve basarsi su standard di sicurezza internazionali riconosciuti.

Gestione Responsabile dei Dati

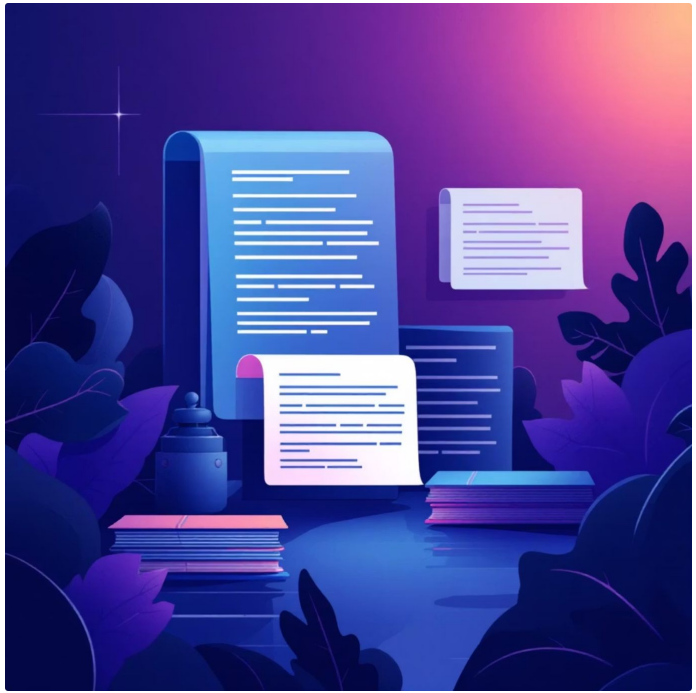
Conformità rigorosa al GDPR e alle normative sulla privacy vigenti.

Prevenzione delle Discriminazioni

I sistemi riducono al minimo i rischi legati ai bias algoritmici.

Ruoli e Responsabilità

Definizione chiara dei ruoli nelle fasi decisionali e di gestione delle soluzioni.



Conformità Normativa e Protezione dei Dati

L'implementazione dell'IA nelle istituzioni scolastiche richiede il rispetto scrupoloso di tutti i requisiti normativi vigenti in materia di protezione dei dati personali.

- Piena conformità al **Regolamento Generale sulla Protezione dei Dati (GDPR)**
- Rispetto del **Codice Privacy italiano** e delle normative settoriali
- Implementazione di **misure tecniche e organizzative** adeguate
- Documentazione completa di tutti i trattamenti di dati effettuati
- **Valutazioni d'impatto (DPIA)** sulla protezione dei dati quando necessario

L'Architettura di un'IA Sicura a



Playbook operativo e strategico per l'adozione dell'IA nel rispetto del GDPR, dell'AI Act e delle Linee Guida MIM 2025. Un'infrastruttura validata che integra Data Privacy, Governance, AI Compliance e allineamento normativo in ogni componente dell'ecosistema scolastico.

FASE INIZIALE

1° Fase: Definizione del Progetto

Prima di implementare soluzioni di IA, l'istituzione scolastica deve effettuare un'attenta analisi preliminare che coinvolga tutta la comunità educativa.

Analisi del contesto

Individuare le aree di applicazione più rilevanti per le specifiche esigenze dell'istituto

Valutazione Benefici e Rischi

Effettuare un'analisi approfondita dei vantaggi attesi e dei potenziali rischi

Fattibilità Organizzativa

Verificare gli strumenti tecnologici disponibili e l'adeguatezza delle infrastrutture

Analisi delle Risorse

Valutare le competenze interne ed eventualmente identificare supporto esterno

Coinvolgimento della Comunità: È fondamentale in questa fase ascoltare docenti, studenti, famiglie e personale per individuare le reali necessità e costruire un'idea progettuale condivisa e partecipata.



Strutturare Piano attuazione integrato al PTOF

LINK AL PIANO

Elementi del Pianodi attuazione

Il piano di attuazione (integrato al PTOF): definisce la strategia didattica e organizzativa dell'istituto, definendo e promuivendo un uso consapevole degli strumenti Ai

01

Definisce le regole basi

Individua i riferimenti normativi e definisce le procedure interne

02

Coordinamento con documenti programmatici

Prevede l'introduzione dell'ai con I documenti programmatici dell'Istituto (Ptov, Rav; Pdm, Atti di indirizzo del DS)

03

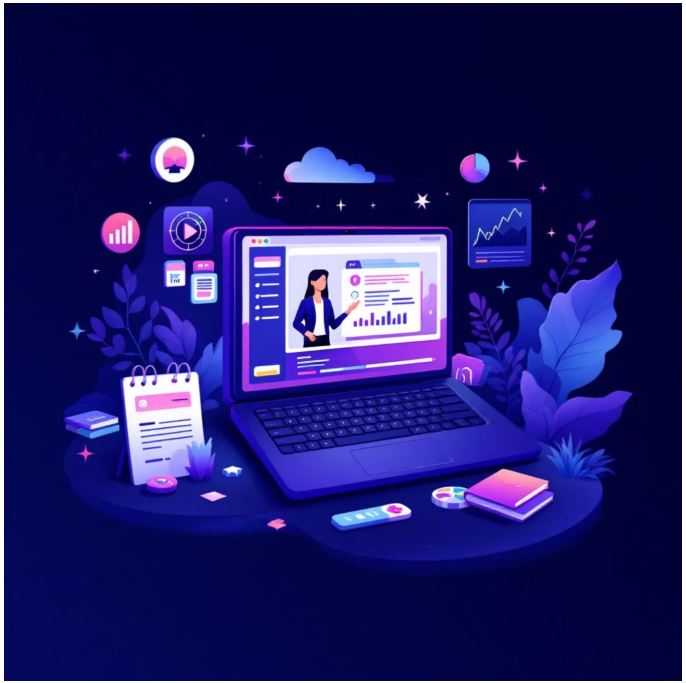
Formazione

Prevede e pianifica una programma formativo per il personale scolastico

04

Costituzione Gruppo di lavoro

Prevede la costituzione del Gruppo di Lavoro



Piattaforme Disponibili: Sfruttare le risorse formative già a disposizione delle istituzioni scolastiche per ottimizzare tempi e costi dell'implementazione.



2° Fase: Pianificazione della struttura e dei ruoli

L'adozione efficace dell'intelligenza artificiale richiede una pianificazione strategica dettagliata che definisca obiettivi chiari, ruoli specifici.

- Costituzione Gruppo di lavoro per Ai
- Individuazione Referente Ai.

Composizione Gruppo lavoro:

- Dirigente scolastico;
- Animatore o team digitale;
- Personale con competenze in materia (docenti, assistenti amministraivi , assistenti tecnici)

	DIRIGENTE SCOLASTICO	DPO/RPD	REFERENTE AI	GRUPPO DI LAVORO	DOCENTI
RESPONSABILITA' LEGALE	X				
VALUTAZIONE SICUREZZA (DPIA)	APPROVA	VALIDA	Supporta e mappa		
COMPITI PRINCIPALE		Supporta il gruppo di lavoro	Fornisce linee guide e coordina il GDL	-Analizza fabisogni; Sperimenta pratiche didattiche	Supervisione didattica:Human in the Loop*
MONITORAGGIO APPLICATIVI			Verifica requisiti tecnici		

* Human in the Loop: l'intervento o la supervisione umana sono integrati nel processo decisionale o operativo di un sistema di Intelligenza Artificiale.



REGOLAMENTO GDPR

Data Protection Officer (DPO): il Ruolo

Il DPO è una figura chiave nel sistema di governance della protezione dei dati personali. Dotato di competenze specialistiche, svolge funzioni di consulenza, controllo e interfaccia istituzionale, operando in piena autonomia e con accesso diretto al vertice aziendale.

1	**Competenza Specialistica**	Possiede **conoscenza approfondita** della normativa GDPR, delle prassi di settore e degli standard tecnici applicabili al trattamento dei dati personali.
2	**Consulenza e Relazioni**	Si relaziona con gli **interessati**, fornisce **consulenza qualificata** al titolare, al responsabile del trattamento e ai dipendenti dell'organizzazione.
3	**Autonomia e Indipendenza**	Opera in piena **autonomia decisionale**, senza ricevere istruzioni vincolanti, ed è **coinvolto in modo tempestivo** in tutte le questioni rilevanti.
4	**Effettua Audit**	Effettua audit in presenza, offre consulenza in ambito giuridico legale anche relativamente all'accesso agli atti .
5	**Verifica dell'Osservanza**	Controlla il **rispetto della normativa**, verifica l'attribuzione delle responsabilità interne, promuove la sensibilizzazione e coordina la formazione del personale.
6	**DPIA e Garante**	Esprime **parere sulla valutazione d'impatto** (DPIA) e ne segue lo svolgimento. Funge da **punto di contatto con il Garante della Privacy** per le attività di vigilanza.



FASE 3

3° Fase: Individuazione delle regole : Redazione Regolamento Ai

L'integrazione effettiva degli strumenti di intelligenza artificiale richiede un approccio graduale, basata sulla definizione delle regole: Redigere Regolamento Ai.

Regole utilizzo per Docenti Assistenti amministrativi e alunni

Stabilire procedure

Subordinare l'utilizzo degli applicativi all'autorizzazione del Ds ovvero alla Valutazione del rischio del DPO

Funzionamento Gruppo lavoro

Stabilire le regole del Gruppo di lavoro:

- Ogni quanto si riunisce;
- Per quali finalita;
- Compiti

Piano formativo

Programmare un piano di formazione per personale:

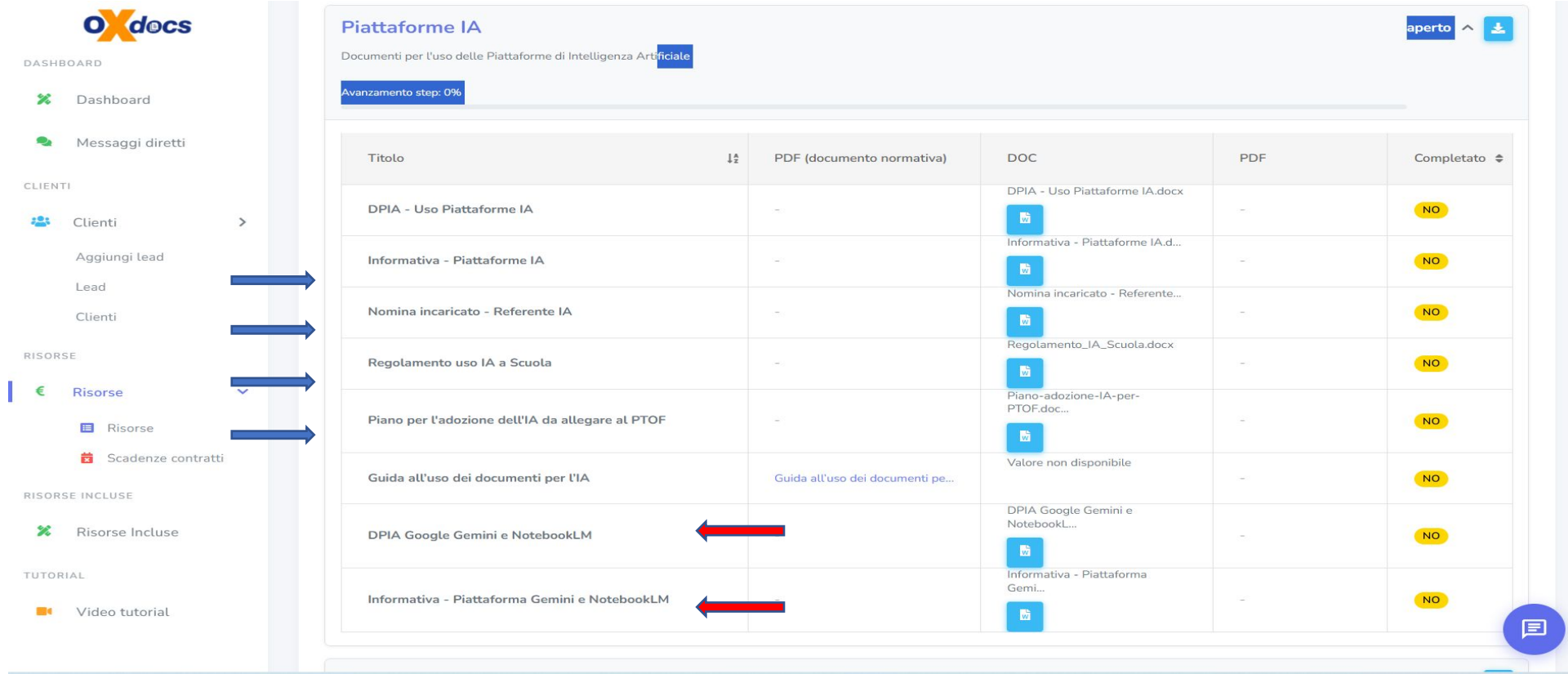
- Strutturare contenuti didattici modulari adatti a diversi livelli di competenza



3° Fase: Garantire trasperenza e chiarezza per gli utilizzatori

L'adozione efficace dell'intelligenza artificiale richiede la predisposizione di informative privacy, una per ogni applicativo utilizzato, specifica per l’utilizzo specific dello strumento.

RICAPITOLIAMO LA DOCUMENTAZIONE



Il Filtro di Conformità per gli



1

Certificazioni di Sicurezza

Requisito obbligatorio: **ISO/IEC 27001**, qualificazione AgID per SaaS. Standard internazionali riconosciuti.

2

Regolamento UE AI Act

Il produttore deve presentare **Dichiarazione di Conformità (Art. 47)** e rispettare le norme armonizzate europee.

3

Protezione Addestramento (LLM)

Blocco assoluto per piattaforme che utilizzano dati e prompt degli studenti per addestrare propri modelli. **Nessuna profilazione ammessa.**

4

Accesso alla Scuola

Solo i produttore che superano ogni filtro ottengono l'accesso all'ecosistema scolastico certificato.

AI ACT — REGOLAMENTO UE 2024/1689

Che fine ha fatto la scadenza del 2 agosto 2026?

Cosa era previsto peri Il **2 agosto 2026** ? La piena applicabilità dell'**AI Act** per i sistemi di intelligenza artificiale classificati come **ad alto rischio**.
I fornitori di questi sistemi dovranno rispettare una serie di obblighi stringenti, tra cui l'obbligo di trasparenza (art. 13): dovranno rilasciare informazioni *concrete, chiare e precise* che includano l'identità del fornitore, le capacità e i limiti del sistema, le specifiche di sicurezza e cybersicurezza, e le modalità della sorveglianza umana — ovvero come il docente può e deve monitorare l'utilizzo dell'IA. Le scuole che adottano tali sistemi dovranno verificare la conformità dei propri strumenti digitali.

Made with GAMMA



Che fine ha fatto la scadenza del 2 agosto?

SISTEMI DI IA AD ALTO RISCHIO

Considerando 56 Ai Act

La diffusione dei sistemi di IA nell'istruzione è importante per promuovere un'istruzione e una formazione digitali di alta qualità e per consentire a tutti i discenti e gli insegnanti di acquisire e condividere le competenze e le abilità digitali necessarie, compresa l'alfabetizzazione mediatica, e il pensiero critico, per partecipare attivamente all'economia, alla società e ai processi democratici. Tuttavia, i sistemi di IA utilizzati nell'istruzione o nella formazione professionale, in particolare per determinare l'accesso o l'ammissione, per assegnare persone agli istituti o ai programmi di istruzione e formazione professionale a tutti i livelli, per valutare i risultati dell'apprendimento delle persone, per valutare il livello di istruzione adeguato per una persona e influenzare materialmente il livello di istruzione e formazione che le persone riceveranno o a cui potranno avere accesso o per monitorare e rilevare comportamenti vietati degli studenti durante le prove, dovrebbero essere classificati come sistemi di IA ad alto rischio, in quanto possono determinare il percorso d'istruzione e professionale della vita di una persona e quindi può incidere sulla sua capacità di garantire il proprio sostentamento. Se progettati e utilizzati in modo inadeguato, tali sistemi possono essere particolarmente intrusivi e violare il diritto all'istruzione e alla formazione, nonché il diritto alla non discriminazione, e perpetuare modelli storici di discriminazione, ad esempio nei confronti delle donne, di talune fasce di età, delle persone con disabilità o delle persone aventi determinate origini razziali o etniche o un determinato orientamento sessuale

Made with GAMMA

SISTEMI AD ALTO RISCHIO NEL CONTESTO SCOLASTICO

Quali tecnologie rientrano nella categoria?

L'AI Act identifica con precisione le categorie di sistemi IA ad alto rischio. Nel contesto scolastico, le seguenti tecnologie richiedono particolare attenzione e piena conformità normativa entro il 2 agosto 2026.



Valutazione e carriera scolastica

Strumenti di valutazione automatizzata che incidono su voti, esami o sull'orientamento dello studente.



Selezione e ammissione

Tecnologie che influenzano l'ammissione, l'assegnazione o la selezione degli studenti a istituti, corsi o specifici percorsi formativi.



Analisi predittiva

Sistemi utilizzati per prevedere il rendimento scolastico o identificare precocemente il rischio di dispersione scolastica.



Monitoraggio negli esami

Software di *proctoring* basati sull'IA per rilevare comportamenti vietati durante le prove d'esame.



Riconoscimento biometrico

Tecnologie biometriche per il controllo delle presenze o per l'analisi comportamentale degli studenti.

Made with GAMMA

AI ACT — REGOLAMENTO UE 2024/1689

Gli obblighi per I Sistemi ad alto rischio



OBBLIGHI DEL FORNITORE

Trasparenza e Conformità: Cosa Deve Garantire il Fornitore

Ai sensi dell'**art. 13 dell'AI Act**, il fornitore deve rilasciare informazioni «concrete, chiare e precise» e redigere una **dichiarazione di conformità UE** che attesti il rispetto dei limiti e delle regole imposte dal regolamento.

1 **Identità del Fornitore**
Nome, sede e dati di contatto del soggetto responsabile del sistema.

2 **Finalità d'Uso**
Descrizione chiara degli scopi per cui l'applicazione è stata progettata e può essere utilizzata.

3 **Capacità e Limiti**
Indicazione esplicita di ciò che il sistema può e non può fare, per un uso consapevole.

4 **Sicurezza e Cybersicurezza**
Specifiche tecniche per prevenire attacchi informatici e proteggere i dati degli utenti.

5 **Sorveglianza Umana**
Modalità con cui il docente può e deve monitorare l'utilizzo dell'IA in classe.

6 **Documentazione Tecnica**
Documentazione completa, conforme e aggiornata, con registrazione nel database UE dei sistemi ad alto rischio.

Made with GAMMA

OBBLIGHI DEL DEPLOYER

Le Responsabilità delle Istituzioni Scolastiche

Le scuole che adottano sistemi di IA ad alto rischio sono **deployer** e devono rispettare precisi obblighi operativi. La responsabilità non è solo del fornitore: l'istituzione scolastica deve agire in modo attivo e documentato.

Verifica e Monitoraggio

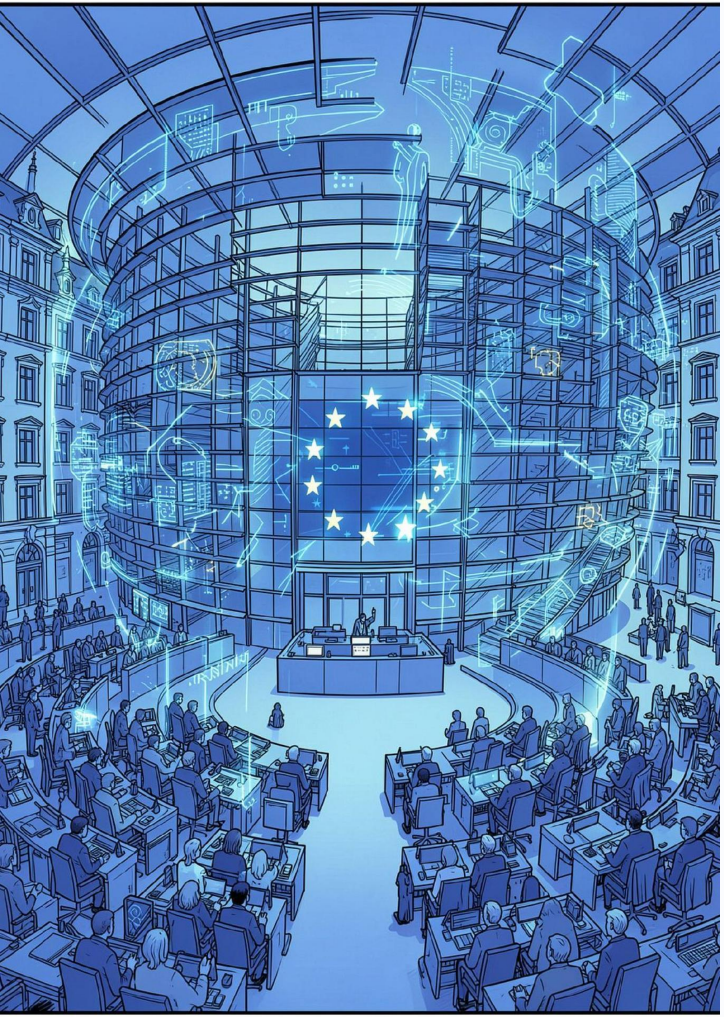
- Verificare la conformità del sistema utilizzato prima dell'adozione
- Monitorare attivamente il funzionamento per intervenire tempestivamente in caso di malfunzionamenti
- Cooperare con l'autorità di vigilanza in caso di controlli

Formazione e Gestione Reclami

- Formare tutto il personale che utilizza sistemi ad alto rischio, garantendo consapevolezza e competenza
- Gestire le segnalazioni e i reclami degli utenti che subiscono un impatto negativo dall'IA
- Mantenere traccia documentale di tutte le attività di monitoraggio e formazione

Attenzione: La mancata conformità può esporre l'istituzione a sanzioni amministrative significative previste dall'AI Act.

Made with GAMMA



DIGITAL OMNIBUS

Il Digital Omnibus e la Nuova Scadenza

Il **Digital Omnibus** è un pacchetto normativo della Commissione Europea che semplifica e unifica la legislazione digitale dell'UE. Una delle modifiche più rilevanti: lo **slittamento degli obblighi per i sistemi ad alto rischio dal 2 agosto 2026 al 2 dicembre 2027**.

Cosa Fare da Settembre: Checklist per le Scuole

01

Mappatura dei Sistemi IA

Censire tutti i software e le tecnologie digitali in uso che integrano funzionalità di IA, sia per la didattica che per la segreteria.

02

Piano d'Istituto sull'IA

Integrare le linee guida sull'uso consapevole dell'IA nel PTOF (Piano Triennale dell'Offerta Formativa).

03

Formazione del Personale

Avviare percorsi formativi mirati per garantire la conformità normativa e prevenire usi distorti dell'IA.

Made with GAMMA

Consiglio dei Ministri, nella seduta n. 177 del 10 giugno 2026

Nuovi Programmi

L'IA entra stabilmente nei curricola del secondo ciclo: aggiornamento delle indicazioni nazionali, IA generativa nei percorsi di studio e integrazione nell'Educazione Civica (etica e cittadinanza digitale).

Formazione Docenti

Piano di formazione stabile su funzionamento, rischi di errore e distorsione, tutela dei dati e uso responsabile dell'IA. Dotazione dedicata: 100 milioni di euro.

Competenze STEAM

Rafforzamento delle competenze in Scienza, Tecnologia, Ingegneria, Arte e Matematica. Orientamento scolastico aggiornato alle trasformazioni tecnologiche e al mercato del lavoro.

Famiglie & Benessere Digitale

Comitati tecnico-etici territoriali a supporto delle scuole. Coinvolgimento attivo delle famiglie per prevenire dipendenze digitali, opacità algoritmica e condizionamento dei minori.

Resta in contatto con noi :

Per informazioni è possibile visitare il nostro sito web - www.oxfirm.it

il servizio PRIVACY :
https://oxfirm.it/adeguamento-gdpr-e-privacy-per-la-scuola/

NEWSLETTER :

https://oxfirm.it/risorse-gratuite/

Resta in contatto con noi :

Per informazioni è possibile visitare il nostro sito web - www.oxfirm.it

la nostra piattaforma documentale : www.oxdocs.it -

→ Scarica la brochure ←

NEWSLETTER :

https://oxfirm.it/risorse-gratuite/

Nuovo cliente :

RICHIEDI LA DEMO DEL PRODOTTO PER 60 GG

https://oxfirm.it/oxdocs-il-software-per-la-gestione-documentale-della-scuola/#calltoaction

Può avere oXdocs **acquistando sul MePA** con i seguenti codici:

OXF-CONS-AT *(licenza annuale)* | **OXF-CONSDOC-AT** *(licenza triennale)*

Grazie della Vostra attenzione

Contatti e Risorse

Per ulteriori informazioni consultare il sito www.oxfirm.it

inviate una mail all'indirizzo oxfirm@oxfirm.it

Oxfirm srl

Sede Legale: Viale Antonio Ciamarra, 259 – 00173 ROMA (RM)

Tel. 06.86356274

Sede Operativa: Piazza Giovanni XXIII, 18 – 81027 San Felice a Cancello (CE)

Tel. 0823 754996

partner Asso Edu

Grazie per l’attenzione

Dr.ssa Maria Aurora Riccardo m.riccardo@oxfirm.it
Rossella Gobbo r.gobbo@oxfirm.it tel. 3482308619