UNIUD
IA POLICY

uniud.it

1	**Premessa**	**p. 03**
1.1	Il contesto normativo e regolamentare	p. 03
1.2	Il contesto accademico	p. 04
2	**La Policy sull'intelligenza artificiale**	**p. 07**
2.1	Principi	p. 07
2.2	Design organizzativo	p. 09
3	**Ambito di applicazione**	**p. 11**
3.1	Ambito di applicazione oggettivo	p. 11
3.2	Ambito di applicazione soggettivo	p. 11
4	**Metodologia adottata nella predisposizione delle linee guida**	**p. 12**
4.1	Approccio 'basato sul rischio' (*risk based*)	p. 12
4.2	Approccio induttivo: individuazione dei 'casi d'uso'	p. 13
4.3	Modello di comunicazione e applicazione delle linee guida	p. 13
5	**Limiti generali all'impiego dei Sistemi di IA**	**p. 15**
6	**Comunità di pratica e UNIUD 'Sandbox'**	**p. 18**
7	**Glossario**	**p. 19**
8	**Riconoscimenti**	**p. 21**

1. Premessa

Sebbene l'Intelligenza Artificiale (IA) esista come autonomo campo di ricerca dal 1955, le rapide evoluzioni degli ultimi anni legate da un lato allo sviluppo tecnologico dei calcolatori elettronici, in particolare in grado di sfruttare algoritmicamente la disponibilità di un elevato parallelismo a basso costo fornito dalle schede GPU programmabili, dall'altro all'accessibilità di quantità di dati inimmaginabile fino a pochi anni fa attraverso la rete Internet e all'accesso quotidiano a questa da parte di miliardi di dispositivi di ogni tipo, hanno permesso una accelerazione dello sviluppo e a una diffusione capillare e generalizzata di strumenti di IA accessibili a tutti, anche gratuitamente. Questa accelerazione ha causato una rivoluzione in molte aree, creando nuove opportunità per il mondo produttivo, della ricerca, della didattica, della amministrazione, ma anche introducendo una serie di rischi e problematiche che necessitano di essere affrontate, comprese e, laddove possibile, normate.

1.1 Il contesto normativo e regolamentare

A livello internazionale sono numerose le iniziative adottate per affrontare il progresso e la diffusione dell'IA, quali ad esempio la Raccomandazione sull'Etica dell'Intelligenza Artificiale da parte dell'UNESCO [1], il 'Global Digital Compact' nell'ambito delle Nazioni Unite [2], la Convenzione Quadro del Consiglio d'Europa sull'Intelligenza Artificiale, i Diritti Umani, la Democrazia e lo Stato di Diritto [3].

I sistemi di intelligenza artificiale sono disciplinati da un quadro normativo complesso e articolato, composto da fonti sia europee sia nazionali che regolano lo sviluppo, l'impiego e la governance delle tecnologie digitali.

Il Regolamento (UE) 2024/1689, noto come 'AI Act' [4], costituisce un quadro normativo organico di disposizioni per lo sviluppo e l'utilizzo dei sistemi di intelligenza artificiale nell'Unione europea ed introduce un approccio basato sul ***rischio***, distinguendo tra Sistemi di IA vietati, sistemi ad alto rischio, sistemi a rischio limitato e sistemi a rischio minimo. Particolare attenzione è riservata nel Regolamento ai sistemi classificati come ad alto rischio, per i quali sono previsti requisiti specifici in materia di qualità dei dati, trasparenza, supervisione umana, sicurezza e responsabilità.

La **Legge 23 settembre 2025, n. 132** [5] – che recepisce e integra a livello nazionale le indicazioni dell'AI Act' – rappresenta per l'Italia il primo quadro normativo organico dedicato all'intelligenza artificiale, definendo i principi generali per lo sviluppo e l'utilizzo dell'IA e promuovendo un impiego delle tecnologie fondato sulla tutela dei diritti fondamentali, sulla trasparenza dei sistemi algoritmici e sulla responsabilità degli operatori. Tale normativa prevede specifiche disposizioni relative all'utilizzo dell'IA all'interno della Pubblica Amministrazione, stabilendo che tali strumenti possano supportare i processi decisionali amministrativi, senza tuttavia sostituire la ***responsabilità umana*** degli operatori.

La normativa specificamente dedicata all'intelligenza artificiale deve necessariamente essere interpretata, contemperata e applicata nel rispetto delle disposizioni vigenti in materia di digitalizzazione della Pubblica Amministrazione, protezione dei dati personali, cybersicurezza e tutela della proprietà intellettuale. Tali fonti delineano, per l'appunto, un sistema di principi e regole volto a orientare l'utilizzo responsabile delle tecnologie di intelligenza artificiale, con particolare attenzione alla tutela dei diritti fondamentali, alla trasparenza e tracciabilità dei sistemi, alla sicurezza e protezione dei dati, nonché alla ***responsabilità delle organizzazioni*** che sviluppano o impiegano tali tecnologie.

Una fonte primaria da tenere in considerazione nell'utilizzo dell'Intelligenza Artificiale è rappresentata dal **Regolamento (UE) 2016/679** (noto come Regolamento Generale sulla Protezione dei Dati, 'GDPR') [6], che disciplina il trattamento dei dati personali. In particolare, nell'utilizzo dei sistemi di intelligenza artificiale non è possibile prescindere dalle disposizioni contenute all'articolo 22 del GDPR, che riconoscono agli interessati il diritto a non essere sottoposti a ***decisioni*** basate ***unicamente su trattamenti automatizzati***, compresa la profilazione, qualora tali decisioni producano effetti giuridici o incidano in modo analogo significativamente sulla persona.

Lo sviluppo e l'utilizzo di sistemi basati su intelligenza artificiale deve, altresì, considerare le disposizioni contenute nel **Codice dell'Amministrazione Digitale (CAD)** (D.Lgs. 82/2005) [7] che stabiliscono i principi generali per la digitalizzazione della Pubblica Amministrazione e riconosce ai cittadini e agli utenti specifici *diritti digitali*, tra cui rientrano il diritto all'uso delle tecnologie nei rapporti con la Pubblica Amministrazione; il diritto alla qualità dei servizi digitali; il diritto all'accessibilità e alla sicurezza delle informazioni.

L'utilizzo di strumenti di intelligenza artificiale deve, inoltre, avvenire nel rispetto della normativa sul diritto d'autore (nel nostro ordinamento, la **Legge 22 aprile 1941, n. 633**) [8]. In particolare, è necessario garantire il rispetto delle disposizioni relative all'utilizzo di opere protette, alla corretta attribuzione della paternità delle opere e alla gestione dei contenuti generati con il supporto di sistemi di intelligenza artificiale.

Infine, l'intelligenza artificiale deve essere inquadrata nell'ambito delle azioni relative alla sicurezza informatica, che comprende da un lato le questioni legate alla 'sovranità digitale', dall'altro quelle concernenti l'organizzazione istituzionale e la cooperazione tra soggetti pubblici e privati, così come stabilito dalla Direttiva (UE) 2022/2555 **'NIS2'**, recepita dal **D.Lgs. 138/2024** [9]. L'estrema mutevolezza del quadro normativo è confermata dal fatto che sia la NIS2 che il **Regolamento (UE) 2019/881 'Cybersecurity Act'** [10] sono, alla data del presente documento, in fase di revisione.

Oltre al quadro più strettamente normativo, un altro aspetto da tenere in considerazione è quello relativo alla rapida innovazione scientifica, che determina misure di sicurezza e approcci organizzativi da adottare sia a livello tecnologico [11] che organizzativo [12].

Ulteriori fonti sono rappresentate da linee guida pubblicate a livello istituzionale, quali quelle elaborate a livello UE [13] e – sebbene non ancora ufficialmente adottate – le Linee guida dell'Agenzia per l'Italia Digitale per l'adozione [14], lo sviluppo [15] e la acquisizione [16] di Sistemi di IA da parte delle Pubbliche Amministrazioni. Tali documenti si propongono di fornire alle amministrazioni pubbliche indicazioni operative relative agli scopi suddetti con particolare riferimento alla valutazione dei rischi, alla trasparenza dei sistemi e alla qualità dei servizi digitali [17].

1.2 Il contesto accademico

L'uso di strumenti di IA può rappresentare una concreta opportunità per le attività di amministrazione universitaria, didattica, ricerca e terza missione, in termini di qualità, efficienza ed efficacia, ma anche consistenti rischi con diversi gradi di probabilità di eventi avversi ed entità dell'impatto e complessità di gestione. Per quanto concerne i benefici, ad esempio, l'IA può favorire lo sviluppo di percorsi di apprendimento adattabili a diverse esigenze, supportando i processi di formazione anche in presenza di disabilità o atipicità cognitive, migliorare l'accessibilità alla formazione e la sperimentazione in ambienti virtuali, potenziare la raccolta l'analisi di dati, rendere più efficiente l'esplorazione dello stato dell'arte, e contribuire alla automazione di diversi processi di analisi anche a livello gestionale. Per quanto riguarda i rischi, già allo stato attuale, qualora l'Ateneo si avvalga di strumenti digitali a supporto dei processi decisionali, è necessario garantire:

· tracciabilità e documentabilità del funzionamento dell'intero processo;
· effettiva supervisione umana;
· possibilità di ricostruire e spiegare i criteri adottati;
· replicabilità del processo decisionale.

Ciò comporta, a maggior ragione, che decisioni quali, a titolo esemplificativo, la formazione di graduatorie, l'ammissione o l'esclusione da corsi o procedure selettive, l'attribuzione di benefici o agevolazioni, non possano essere affidate esclusivamente a sistemi automatizzati.

Note

1 Raccomandazione sull'Etica dell'Intelligenza Artificiale del 23 novembre 2021
↳ **Leggi**

2 Il documento è parte del 'Patto per il Futuro', adottato nell'assemblea generale del 22 settembre 2024 (A/RES/79/1)
↳ **Pact for the future**
↳ **Global Digital Compact**

3 Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225), del 5 settembre 2024
↳ **Leggi**

4 Regolamento (UE) 2024/1689 del 13 giugno 2024, in GUUE L, 2024/1689, 12.7.2024
↳ **Leggi**

5 Legge 23 settembre 2025, n. 132, Disposizioni e deleghe al Governo in materia di intelligenza artificiale, GU n.223 del 25-09-2025
↳ **Leggi**

6 Regolamento (UE) 2016/679 del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE, in GU L 119 del 4.5.2016, pagg. 1-88
↳ **Leggi**

7 Decreto Legislativo 7 marzo 2005, n. 82, Codice dell'amministrazione digitale, in GU n.112 del 16 maggio 2005 – Suppl. Ordinario n. 93
↳ **Leggi**

8 Legge 22 aprile 1941, n. 633, Protezione del diritto d'autore e di altri diritti connessi al suo esercizio, in GU n.166 del 16-07-1941
↳ **Leggi**

9 Decreto Legislativo 4 settembre 2024, n. 138, Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148, in GU n.230 del 01-10-2024
↳ **Leggi**

10 Regolamento (UE) 2019/881 del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 ('Regolamento sulla cibersicurezza') in GUUE L 151 del 7.6.2019
↳ **Leggi**

11 ISO/IEC TR 24028:2020 Information technology – Artificial intelligence (AI) – Overview on trustworthiness in artificial intelligence
↳ **ISO/IEC TR 24028:2020**

ISO/IEC TR 24027:2021 Information technology – Artificial intelligence (AI) – Bias in AI systems and AI aided decision making
↳ **ISO/IEC TR 24027:2021**

ISO/IEC 38507:2022 – Information technology – Governance of IT – Governance implications of the use of artificial intelligence by organizations
↳ **ISO/IEC 38507:2022**

ISO/IEC 23053:2022 Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML)
↳ **ISO/IEC 23053:2022**

ISO/IEC 23894:2023 – Information technology – Artificial intelligence – Guidance on risk management
↳ **ISO/IEC 23894:2023**

ISO/IEC 42001:2023 – Information technology – Artificial intelligence – Management system
↳ **ISO/IEC 42001:2023**

ISO/IEC 5338:2023 – Information technology – Artificial intelligence – AI system life cycle processes
↳ **ISO/IEC 5338:2023**

ISO/IEC TR 5469:2024 Artificial intelligence – Functional safety and AI systems
↳ **ISO/IEC TR 5469:2024**

ISO/IEC 42005:2025 Information technology – Artificial intelligence (AI) – AI system impact assessment
↳ **ISO/IEC 42005:2025**

12 ↳ **AI Risk Management Framework**

13 MEDAGLIA, R., MIKALEF, P. and TANGI, L., Competences and governance practices for artificial intelligence in the public sector, Publications Office of the European Union, Luxembourg, 2024
↳ **Leggi**
↳ **JRC Publications**

14 Linee guida per l'adozione dell'intelligenza artificiale nella Pubblica Amministrazione, Determinazione 17/2025
↳ **Leggi**

15 Linee guida per lo sviluppo dell'intelligenza artificiale nella Pubblica Amministrazione, Determinazione 43/202
↳ **Leggi**

16 Linee guida per il procurement di IA nella Pubblica Amministrazione, Determinazione 43/2026
↳ **Leggi**

17 **Vi sono inoltre documenti di programmazione rispetto a cui deve essere coerente l'implementazione dell'IA all'interno di una PA, come il Piano Integrato di Attività e** Organizzazione (PIAO) di cui al Decreto-Legge 9 giugno 2021, n. 80, Misure urgenti per il rafforzamento della capacità amministrativa delle pubbliche amministrazioni funzionale all'attuazione del Piano nazionale di ripresa e resilienza (PNRR) e per l'efficienza della giustizia
↳ **Leggi**

2. La Policy sull'intelligenza artificiale

L'Università degli Studi di Udine intende dotarsi di una disciplina che possa coniugare i valori enunciati e i principi espressi nel suo Statuto, nonché le disposizioni interne comprensive dei Regolamenti sull'integrità della ricerca e del Codice etico, in relazione all'utilizzo dell'IA all'interno della comunità universitaria e nei confronti delle altre istituzioni con i seguenti obiettivi:

· Assicurare una corretta informazione di base, promuovere opportunità di aggiornamento e incentivare azioni volte ad aumentare la consapevolezza sull'uso dello strumento.

· Promuovere e sostenere iniziative di formazione all'uso dei sistemi di AI a beneficio delle studentesse e degli studenti, del personale docente, delle collaboratrici e collaboratori didattici, del personale ricercatore, e del personale tecnico amministrativo.

· Sostenere e accogliere l'utilizzo dei sistemi di AI nelle attività di didattica e di ricerca e della loro valorizzazione nel fermo rispetto dei principi qui indicati.

· Favorire il coinvolgimento della comunità universitaria, per condividere le migliori pratiche alla luce dei costanti aggiornamenti della tecnologia e della sua applicazione, anche al fine di aggiornare le indicazioni del presente documento, intercettare nuove esigenze formative e comprendere quale tipo di supporto potrebbe essere più utile.

2.1 Principi

Nel perseguire tali obiettivi, ci si propone di osservare i seguenti principi:

Etico-relazionale

1 Centralità della persona

L'intelligenza artificiale è uno strumento al servizio della persona. La dignità, l'autonomia e i diritti fondamentali degli individui costituiscono il limite invalicabile di qualsiasi applicazione dell'IA, a prescindere dai 'livelli di autonomia' di cui i sistemi possono essere dotati.

2 Responsabilizzazione 'accountability'

L'uso dell'IA richiede consapevolezza critica, capacità di valutazione e disposizione attiva al controllo dei risultati. La responsabilizzazione è un processo continuo che coinvolge l'intera comunità accademica.

3 Trasparenza e tracciabilità

Quando un risultato dell'utilizzo di strumenti di IA è rilevante per il contenuto o il significato tale utilizzo deve essere riconoscibile e dichiarato, consentendo a terzi di valutare l'origine e la natura dei contenuti prodotti.

Tecnico-giuridico

4 Accuratezza e qualità dell'informazione

I contenuti generati dall'IA non costituiscono fonti affidabili in sé. La verifica critica degli output e la qualità delle informazioni fornite in input sono condizioni necessarie per un uso responsabile.

5 Protezione dei dati e sicurezza

L'uso dell'IA deve avvenire nel rispetto della riservatezza delle persone e della sicurezza delle informazioni, siano esse personali, riservate o strategiche per l'istituzione.

6 Proprietà intellettuale e copyright

L'uso dell'IA non deve ledere i diritti di autori e creatori, né esporre a rischio il patrimonio intellettuale dell'Ateneo. I prodotti generati possono incorporare opere altrui o contenere informazioni riservate di terzi e i prompt potrebbero fornire al sistema di IA dati che dovrebbero rimanere riservati.

Equità e integrità

7 Equità, inclusione e non discriminazione

L'IA non deve introdurre né amplificare disuguaglianze, pregiudizi o discriminazioni. Il suo impiego deve garantire pari opportunità di accesso e di trattamento per tutti i membri della comunità accademica.

8 Integrità accademica ed etica

L'uso dell'IA deve essere compatibile con i valori fondanti della vita accademica: onestà intellettuale, originalità del pensiero, rigore nella produzione della conoscenza.

Sostenibilità sistemica

9 Sostenibilità ambientale

L'uso dell'IA comporta un impatto ambientale significativo. L'Ateneo promuove un impiego proporzionato e consapevole, orientato a minimizzare i costi energetici e ambientali delle tecnologie adottate.

10 Proattività

L'approccio all'IA deve consentire alla comunità universitaria di essere non solo pronta ma anche proattiva rispetto ai cambiamenti e alle innovazioni che si verificheranno in futuro, promuovendo la cultura dell'innovazione, l'apprendimento collettivo e la sperimentazione in ambienti protetti.

2.2 Design organizzativo

Nell'operare secondo i principi funzionali di cui sopra, l'Università degli Studi di Udine adotta un modello organizzativo caratterizzato come segue e come schematizzato nella figura 1 e riassunto nei successivi otto punti.

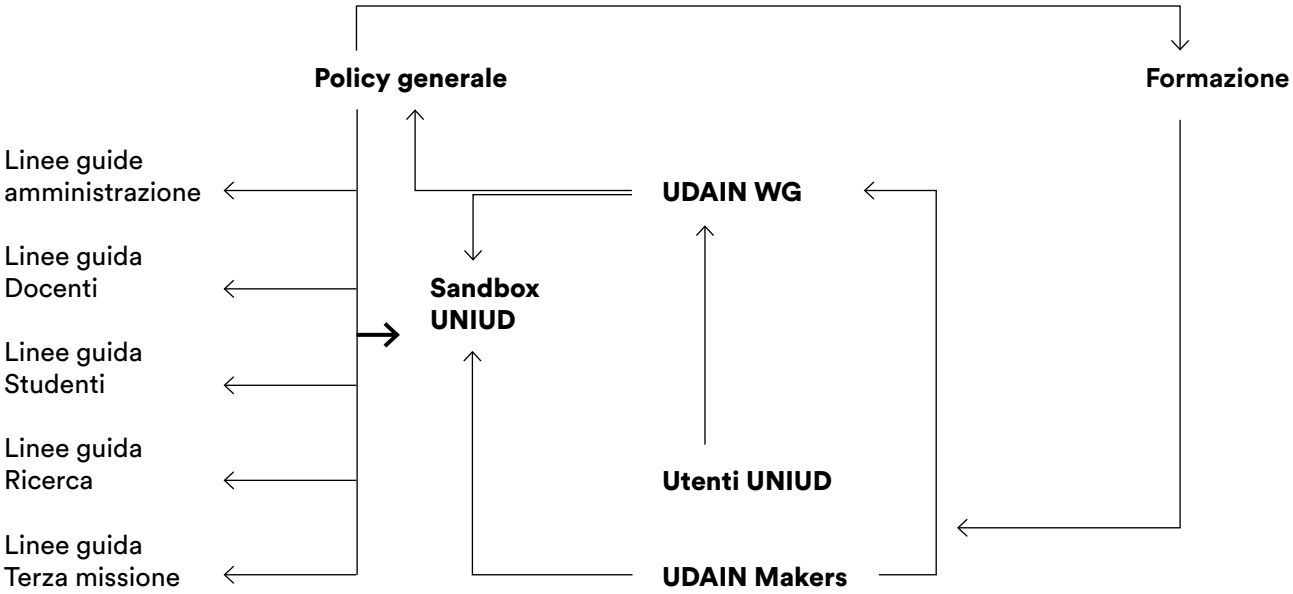


Figura 1
Design organizzativo AI Policy UNIUD

1. Perimetro applicativo esteso: i 'Sistemi di IA'

La Policy si applica a tutti i Sistemi di IA utilizzati nell'Ateneo, indipendentemente dalla loro natura generativa o meno. La definizione di 'sistema di IA' adottata è quella dell'AI Act (art. 3, Reg. UE 2024/1689), così come riportata nel ↳ **Glossario**. L'approccio complessivo è 'tecnologicamente neutrale': nessuna tecnologia specifica è esclusa a priori, nessuna è privilegiata.

2. Struttura 'modulare' a due livelli con aggiornamento differenziato

La Policy generale è declinata nelle linee guida settoriali. La Policy contiene i principi e l'impostazione di fondo ed è soggetta ad approvazione formale degli organi di governo; le linee guida settoriali, che includono le indicazioni operative, sono aggiornabili con procedura semplificata su proposta del gruppo di lavoro di cui al punto 4.

3. Classificazione degli usi per livello di rischio

Ogni uso dell'IA nell'Ateneo è classificato in quattro diversi livelli di rischio (Inaccettabile, Alto, Limitato, Minimo), a cui corrispondono misure proporzionate di supervisione, documentazione e valutazione d'impatto.

4. Istituzione di un gruppo di lavoro dedicato

Con separato provvedimento viene nominato un gruppo di lavoro (*Working Group*) dedicato. Esso ha il compito di mantenere un inventario dei Sistemi di IA adottati, monitorare il loro utilizzo, promuovere l'aggiornamento delle linee guida e la predisposizione delle valutazioni di rischio, qualora richieste. Ha composizione interdisciplinare ed è l'elemento dinamico dell'approccio proattivo adottato dall'Ateneo.

5. Creazione di una community interna

L'Università degli Studi di Udine promuove l'innovazione attraverso la creazione di un canale collaborativo interno aperto a tutte le componenti dell'Ateneo. Il suo funzionamento e la sua gestione sono mantenuti deliberatamente informali per promuovere la più ampia partecipazione e lo scambio trasversale di esperienze.

6. Non c'è responsabilità individuale senza *accountability* istituzionale

La responsabilità sull'uso dei Sistemi di IA rimane in capo al singolo individuo; tuttavia, l'Ateneo determina le condizioni con cui ciò avviene, anzitutto in termini di inquadramento, attribuzioni e formazione, in modo che i principi sopra enunciati diventino criteri operativi di immediata applicazione.

7. Tutela del benessere e accessibilità come diritti

Le linee guida settoriali contengono anche disposizioni specifiche per tutelare il benessere degli utenti e integrano principi e indicazioni per utilizzare l'IA come tecnologia assistiva per personale o studenti con disabilità.

8 Ambiente di sperimentazione istituzionalizzato

Con separato provvedimento l'Ateneo si dota un ambiente controllato (c.d. *sandbox* interna) per consentire la sperimentazione di Sistemi di IA con l'assistenza di personale qualificato e l'eventuale supervisione del *Working Group*.

3. Ambito di applicazione

La presente Policy si applica esclusivamente all'interno del contesto della comunità universitaria e in relazione a due criteri cumulativi: (1) oggettivo, (2) soggettivo.

3.1 Ambito di applicazione oggettivo

La presente Policy si applica ai 'Sistemi di Intelligenza Artificiale' come definiti nel ↳ **Glossario**.

Con ciò si è inteso individuare delle caratteristiche funzionali che determinano la classificazione di un artefatto digitale come 'Sistema di IA' non tanto sulla base delle tecnologie impiegate, quanto per le capacità operative – in particolare i 'diversi gradi di autonomia' di cui esso può disporre.

La presente Policy, in altri termini, si applica laddove un 'Sistema di IA' sia impiegato per compiti riguardanti le attività svolte nel perseguimento delle finalità dell'Università, in qualsiasi modalità e con qualsiasi supporto, formato, protocollo, piattaforma o servizio si possa configurare il suo utilizzo.

3.2 Ambito di applicazione soggettivo

La Policy si applica a tutti i soggetti che appartengono alla comunità universitaria, in modo differenziato a seconda del ruolo ricoperto. Ci si rivolge in particolare a:

· **personale docente** con cui si identificano coloro che svolgono attività didattica o valorizzazione della stessa;

· **collaboratrici e collaboratori didattici** con cui si identificano coloro che collaborano all'erogazione didattica e valorizzazione della stessa (ad esempio tutor didattici);

· **studentesse e studenti** che partecipano a percorsi formativi di primo, secondo o terzo ciclo, o ciclo unico, alle scuole di specializzazione, ai master, a corsi di perfezionamento, ai corsi di formazione insegnanti, ai corsi minor, alle attività complementari, alle scuole (per esempio, *winter* e *summer schools*), ai corsi superiori, ai corsi di formazione continua;

· **personale ricercatore** con cui si identificano coloro che svolgono attività di ricerca e valorizzazione della stessa a prescindere dalla qualifica o dall'inquadramento e dal fatto che l'attività sia svolta a tempo pieno o parziale, ovvero a tempo indeterminato o determinato;

· **personale tecnico amministrativo** così come definito dal Contratto Collettivo del settore ovvero coloro i quali, a prescindere dalla qualifica o dall'inquadramento e dal fatto che l'attività sia svolta a tempo pieno o parziale, ovvero a tempo indeterminato o determinato, operano nelle aree biblioteche, tecniche o amministrative dell'Ateneo, compresi i collaboratori linguistici.

La presente Policy **non si applica** all'utilizzo di tecnologie che non ricadono nell'ambito della definizione di 'Sistema di IA' sopra precisata né qualora l'utilizzo si svolga per finalità personali o comunque estranee all'ambito universitario.

4 Metodologia adottata nella predisposizione delle linee guida

Nella presente sezione si approfondisce l'approccio complessivo con cui la Policy è stata concepita, fornendo alcuni cenni sulle sue basi teoriche, sulla articolazione delle linee guida, sulla classificazione delle singole attività e sulla qualificazione dei rischi ad esse associati. L'obiettivo metodologico è quello di evitare, da una parte, la formulazione di precetti generali di difficile applicazione e, dall'altra, l'elencazione di scenari o 'casi d'uso' troppo dettagliati o dispersivi.

La metodologia adottata si articola su tre aspetti che di seguito vengono brevemente spiegati: (1) approccio 'basato sul rischio' in relazione alle misure di sicurezza; (2) approccio 'induttivo' rispetto all'individuazione dei casi d'uso; (3) definizione di un modello di comunicazione e applicazione delle linee guida.

4.1 Approccio 'basato sul rischio' (*risk based*)

L'Università degli Studi di Udine con la presente Policy si propone di recepire i modelli di regolamentazione più avanzati, prevedendo una disciplina proporzionata al livello di rischio individuato e idonea ad essere implementata nell'organizzazione interna. In questo senso si prende ispirazione dalle Linea guida AGID, nelle quali si fa riferimento alle norme ISO per la gestione dei rischi inerenti l'IA, in particolare la ISO/IEC 23894/2023 [18]. Sempre dalle Linee guida AGID [19] sono riprese le indicazioni relative alla terminologia impiegata nelle formulazioni delle indicazioni [20]. In questo modo sono individuate **quattro categorie** di rischio: (1) **rischio inaccettabile** (colore rosso), che corrisponde a pratiche tecnologiche vietate; (2) **rischio alto**, riferito ad attività che devono essere svolte con misure di sicurezza elevate (colore arancione); (3) **rischio limitato**,corrispondente ad attività da svolgere con misure di sicurezza specifiche (colore giallo); (4) **rischio minimo**,che prevede adeguate misure di sicurezza (colore verde).

I rischi non sono formulati in generale, ma con riferimento a specifiche attività che prevedono l'impiego di Sistemi di IA e che vengono classificate all'interno delle quattro categorie indicate. A seconda della loro classificazione, si prevedono misure di sicurezza crescenti, individuate in modo sistematico e dettagliatamente descritte all'interno delle Linee guida.

Le misure di sicurezza possono essere tecnologiche ed organizzative. In questo secondo senso possono prevedere, in generale o caso per caso, a seconda delle circostanze individuate nella Policy, il coinvolgimento di organismi interni [21] o definiti sulla base della presente Policy (quali il gruppo di lavoro definito al punto 2.2.4.

Rischio Classificazione ripresa dall'AI ACT	**Formulazione linguistica** AGID / ISO	**Colore**	**Misure di sicurezza**
Inaccettabile	Non deve, Non devono Non può, Non possono	Rosso 🔴	Pratiche tecnologiche vietate
Alto	Deve, Devono	Arancione 🟠	Misure di sicurezza **elevate**
Limitato	Dovrebbe, Non dovrebbe	Giallo 🟡	Misure di sicurezza **specifiche**
Minimo	Può o possono o l'aggettivo opzionale	Verde 🟢	Misure di sicurezza **adeguate**

La violazione delle indicazioni contenute nelle Linee guida potrà comportare sanzioni disciplinari ed una eventuale rivalsa da parte dell'Ateneo, oltre all'adozione delle misure ritenute più idonee a tutela dello stesso.

4.2 Approccio induttivo: individuazione dei 'casi d'uso'

Nell'individuazione dei 'casi d'uso' o 'scenari' si fa riferimento ai possibili utilizzi di Sistemi di IA all'interno del contesto sopra individuato mediante le due dimensioni (ambito 'oggettivo' e 'soggettivo'). I 'casi d'uso' sono concepiti assumendo che ciascun componente della comunità universitaria (si veda ↳ **Sezione 3.2**) svolga attività che comportano in qualche modo l'elaborazione di una forma di 'conoscenza', termine che comprende generalmente dati e informazioni relativi ad aspetti indifferentemente astratti o concreti.

4.3 Modello di comunicazione ed applicazione delle linee guida

La comunicazione delle linee guida è articolata in più documenti a seconda del **contesto** al quale si riferiscono, ai **destinatari** a cui si rivolgono e al livello di **rischio**.

Nella tabella che segue si indica l'assegnazione dei codici in relazione all'ambito.

Codice delle linee guida	Ambito di applicazione
G	Linee guida generali, contenute nel presente documento
A	Amministrazione, rivolte principalmente al personale tecnico amministrativo dell'indicazione
D	Didattica, rivolte principalmente ai docenti
R	Ricerca
S	Didattica, indirizzate agli studenti
T	Terza missione, valorizzazione della conoscenza

Nella tabella che segue si indica l'assegnazione dei codici in funzione del rischio.

Codice del livello di rischio	Ambito di applicazione	Indicazione grafica
V	Attività vietata	🔴 VIETATO
A	Attività ad alto rischio	🟠 ALTO RISCHIO
L	Attività a rischio limitato	🟡 LIMITATO
M	Attività a rischio minimo	🟢 MINIMO

Nella tabella che segue si riporta la struttura della singola indicazione.

Identificatore dell'indicazione	**Titolo dell'indicazione**	**Descrizione dell'attività**	**Livello di rischio**
Codice e numero identificativo dell'indicazione	Denominazione sintetica	Breve descrizione dell'attività a cui l'indicazione fa riferimento	Colore (sfondo rosso, arancione, giallo, verde) e corrispondente indicazione (proibito, elevato, limitato, minimo

Le singole indicazioni possono essere corredate da ulteriori dettagli, che hanno lo scopo di descrivere ulteriormente la specifica attività considerata; fornire spiegazioni e approfondimenti, anche con l'ausilio di schemi o grafici, sui rischi individuati; talora indicare le misure di sicurezza da adottare.

Note

18 ISO/IEC 23894:2023 Information technology – Artificial intelligence (AI) – Guidance on risk management
↳ **ISO/IEC 23894:2023**

19 DEVE o DEVONO indicano un requisito obbligatorio; NON DEVE o NON DEVONO o NON PUÒ o NON POSSONO indicano un assoluto divieto; DOVREBBE o NON DOVREBBE indicano che le implicazioni devono essere comprese e attentamente pesate prima di scegliere approcci alternativi; PUÒ o POSSONO o l'aggettivo OPZIONALE indica che il lettore può scegliere di applicare o meno la specifica

20 Verbal forms for expressions of provisions
↳ **Leggi**

21 Ad esempio: Chief Information Security Officer (CISO), Responsabile per la Protezione dei Dati Personali (c.d. 'Data Protection Officer' o DPO, Responsabile per la Transizione Digitale (RDT)

5 Limiti generali all'impiego dei Sistemi di IA

Determinate tipologie di impiego dei Sistemi di IA presentano criticità tali da rendere necessario un divieto formale al loro utilizzo. In questa sezione se ne evidenziano alcune, ritenute fondamentali riassunte dalla seguente tabella di sintesi.

Identificatore dell'indicazione	Indicazione dell'attività di sintesi	Descrizione dell'attività	Classificazione per livello di rischio
GV01	Uso di sistemi completamente autonomi senza supervisione	Uso di funzionalità o sistemi che senza alcuna forma di monitoraggio, supervisione o controllo umano	VIETATO 🔴
GV02	Trattamento di informazioni confidenziali	Uso di Sistemi di IA per trattare documenti contenenti informazioni confidenziali, know-how, segreti industriali, segreto d'ufficio, in tema di accesso amministrativo o altro	VIETATO 🔴
GV03	Trattamento di materiale in violazione del diritto d'autore	Uso di Sistemi di IA per elaborare materiale (testi, audio, video, immagini) in violazione della licenza sull'utilizzo o della normativa	VIETATO 🔴
GV04	Elaborazione di dati personali	Uso di IA per trattare documenti contenenti dati personali	VIETATO 🔴

Si sottolinea che le indicazioni sopra riportate hanno valenza generale, sicché operano se e in quanto non prevalgano indicazioni più specifiche contenute nelle linee guida speciali.

GV01 — Uso di sistemi completamente autonomi senza supervisione

Le funzionalità 'agentic' (cfr. 'Agentic AI', ↳ **Glossario**) configurano un profilo di rischio strutturalmente incompatibile con i requisiti di supervisione umana imposti dall'AI ACT' (Reg. (UE) 2024/1689, L. 132/2025) e dalla normativa sulla digitalizzazione della Pubblica Amministrazione (D.Lgs. 82/2005, c.d. 'CAD').

La ragione fondamentale del divieto risiede nell'imputazione dell'attività svolta: quando un Sistema di IA opera autonomamente su risorse dell'Ateneo – accedendo a file, inviando comunicazioni, eseguendo operazioni su sistemi informativi – diventa oggettivamente impossibile mantenere un'effettiva *accountability* sui processi ed in particolare garantire la replicabilità del processo decisionale o la ricostruibilità dei criteri adottati. Si tratta dei requisiti minimi che la Policy stessa individua come precondizione per qualsiasi uso di strumenti digitali a supporto dei processi decisionali.

Sul piano della sicurezza informatica, l'inserimento di credenziali istituzionali in Sistemi di IA di terze parti trasferisce all'esterno dell'Ateneo il controllo su risorse e accessi propri dell'istituzione, con

rischi gravi la cui mitigazione non è verificabile anche in presenza di specifiche garanzie contrattuali. Questo profilo interseca le prescrizioni della Direttiva NIS2 (recepita dal D.Lgs. 138/2024) in materia di sicurezza delle reti e dei sistemi informativi degli enti pubblici, che richiedono misure organizzative e tecniche proporzionate alla natura delle risorse trattate.

Il divieto **non esclude** che **specifiche modalità** di impiego 'agentic' possano essere autorizzate in contesti controllati – tipicamente all'interno della UNIUD Sandbox – previa valutazione del rischio e con la supervisione del Working Group. In assenza di un quadro valutativo consolidato, l'estensione del perimetro di azione autonoma dei Sistemi di IA all'infrastruttura istituzionale è incompatibile con il principio 'Non c'è responsabilità individuale senza accountability istituzionale'.

GV02 — Trattamento di informazioni confidenziali

L'Ateneo nell'esercizio dei suoi compiti istituzionali detiene informazioni confidenziali, intendendo con ciò dati che comprendono sia 'segreti d'ufficio' ai sensi del diritto amministrativo che 'segreti commerciali' ai sensi del diritto industriale, cfr. ↳ **Glossario**). Il divieto di impiegare Sistemi di IA per trattare tali dati trae fondamento da una pluralità convergente di norme e principi.

Il caricamento di tali informazioni da parte di un dipendente – anche attraverso la semplice inclusione in un prompt (cfr. ↳ **Glossario**) – nei Sistemi di IA gestiti da soggetti terzi non autorizzati dal detentore può integrare una copia non autorizzata.

Ciò deriva dal fatto che negli LLM (cfr. ↳ **Glossario**) i dati di input vengono impiegati per l'addestramento dei modelli, anche attraverso la memorizzazione temporanea su server esterni, e possono essere potenzialmente resi disponibili a terzi.

Il divieto integra i principi espressi nell'ambito n.5 (↳ **Protezione dei dati e sicurezza**) e n.6 (↳**Proprietà intellettuale e copyright**).

La riservatezza non è, in questa prospettiva, un vincolo meramente formale (incorporato nella 'modulistica'), o gestionale (sanzionato nelle procedure organizzative) ma una componente funzionale dell'interazione tra la singola persona e l'infrastruttura digitale.

GV03 — Trattamento di materiale in violazione del diritto d'autore

Il divieto riguarda l'utilizzo di Sistemi di IA per elaborare materiale in qualsiasi formato e di qualsiasi natura – testi, audio, video, immagini – in violazione della vigente disciplina sul diritto d'autore.

Il divieto è giustificato sotto due aspetti:

· **L'input**: inserire in un sistema di IA un testo protetto da copyright per elaborarlo (riassunto, traduzione, trasformazione) può costituire un atto di riproduzione non autorizzata, a meno che la licenza dell'opera lo consenta espressamente.

· **L'output**: i contenuti generati dagli LLM possono incorporare, in modo non trasparente e non percepibile da parte dell'utente, porzioni di opere protette presenti nei dati di addestramento, con il rischio di esporre l'Ateneo a responsabilità per violazione di copyright nei confronti di autori terzi.

La tutela del patrimonio intellettuale dell'Ateneo – che include le opere prodotte dai propri docenti e ricercatori – è parte integrante del principio numero 6, che specifica come 'l'uso dell'IA non deve ledere i diritti di autori e creatori, né esporre a rischio il patrimonio intellettuale dell'Ateneo'.

Il divieto non impedisce l'utilizzo di IA su materiale per il quale si dispone di licenza compatibile o che è di pubblico dominio: in questi casi si rientra nelle fattispecie disciplinate dalle linee guida settoriali.

GV04 — Elaborazione di dati personali

La disciplina del trattamento dei dati personali prevede che qualsiasi trattamento di dati personali abbia una base giuridica specifica (artt. 6 e 9 GDPR), sia fondato, tra gli altri, sul principio di minimizzazione (art. 5, lett. c) GDPR), avvenga con misure di sicurezza adeguate (art. 32 GDPR) e non produca decisioni basate unicamente su trattamenti automatizzati con conseguenze economiche o giuridiche significative nei confronti degli interessati (art. 22 GDPR). Soprattutto quando i dati personali sono inseriti in Sistemi di IA commerciali di terze parti (es: ChatGPT, Claude, Gemini), il rispetto di tali prescrizioni è problema-

tico in quanto il titolare del trattamento non ha un effettivo controllo sulla loro architettura, politica di conservazione e modalità di trattamento.

In ambito universitario i dati trattati includono categorie particolari ai sensi dell'art. 9 GDPR (es: situazioni di disabilità, condizioni di salute, orientamento politico nelle attività studentesche, e dati relativi a procedimenti disciplinari o selettivi). L'inserimento anche involontario di tali dati in un 'prompt' può determinare una potenziale violazione nella sicurezza (c.d. 'data breach') con obbligo di notifica al Garante ai sensi dell'art. 33 GDPR entro 72 ore dall'accertamento.

Il divieto rafforza quanto previsto dal Regolamento interno dell'Ateneo in materia di protezione dei dati personali (emanato con D.R. n. 182 del 13 marzo 2023) nel quale si stabiliscono obblighi specifici per gli autorizzati al trattamento e procedure di gestione delle violazioni.

Con ciò **non si esclude** che dati personali possano essere trattati con Sistemi di IA nelle condizioni stabilite dalle **linee guida** settoriali e con **adeguate garanzie**.

6 Comunità di pratica e UNIUD 'Sandbox'

L'Università degli Studi di Udine riconosce che un uso responsabile dell'intelligenza artificiale non si costruisce per via individuale, ma richiede processi condivisi di apprendimento, confronto e aggiornamento continuo. La rapidità dell'evoluzione tecnologica e la varietà dei contesti applicativi rendono insufficiente un approccio puramente normativo: accanto alle regole, occorrono spazi istituzionali in cui la conoscenza possa circolare, le esperienze essere capitalizzate e le criticità affrontate collettivamente prima che diventino problemi sistemici.

A tal fine, l'Ateneo istituisce **due strumenti complementari**: una comunità di pratica, per alimentare la riflessione collettiva; una 'sandbox', per consentire, in condizioni controllate, la verifica empirica di nuovi strumenti o applicazioni.

La 'comunità di pratica' sull'IA, aperta a tutte le componenti della comunità accademica – docenti, ricercatori, personale tecnico-amministrativo e studenti – quale luogo permanente di scambio di esperienze, elaborazione di buone pratiche e riflessione critica sugli usi emergenti degli strumenti di IA, non ha funzione prescrittiva, ma opera come motore dell'apprendimento organizzativo: raccoglie evidenze dall'uso reale, ne valuta le implicazioni e contribuisce all'aggiornamento periodico delle presenti linee guida.

La cosiddetta 'sandbox' istituzionale è un ambiente di sperimentazione controllata nella quale è possibile testare nuovi strumenti e casi d'uso in condizioni di sicurezza, prima di un'adozione estesa nell'ambito delle attività didattiche, di ricerca e amministrative. La 'sandbox' consente di valutare la conformità degli strumenti ai principi delle presenti linee guida, di identificare rischi non previsti e di definire le condizioni di un eventuale impiego più ampio, riducendo l'esposizione dell'Ateneo e delle persone coinvolte. L'istituzione della comunità di pratica e della 'sandbox', nonché la disciplina operativa della 'sandbox' – requisiti di accesso, procedure di valutazione, criteri di approvazione degli strumenti testati e modalità di rendicontazione – sono demandate a un **apposito provvedimento attuativo**.

7 Glossario

Agentic AI
Applicazione dell'intelligenza artificiale con 'autonomia aperta'. Con tale espressione si intende indicare in generale l'approccio che si propone di rendere i Sistemi di IA in grado di stabilire o affinare piani ed eseguire azioni con sorveglianza umana minima o assente (cfr. 'Systemic Risks Associated with Agentic AI: A Policy Brief') [22].

Cibersicurezza
L'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche (cfr. art 2(1), 'Cybersecuriry Act').

Dato personale
Qualsiasi informazione riguardante una persona fisica identificata o identificabile ('interessato'); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (cfr. art. 4(1) GDPR).

Informazioni confidenziali
Informazioni qualificabili come segreto d'ufficio o come segreto commerciale (cfr. art. 15 D.P.R. 3/1957: 'L'impiegato deve mantenere il segreto d'ufficio. Non può trasmettere a chi non ne abbia diritto informazioni riguardanti provvedimenti od operazioni amministrative, in corso o concluse, ovvero notizie di cui sia venuto a conoscenza a causa delle sue funzioni, al di fuori delle ipotesi e delle modalità previste dalle norme sul diritto di accesso'; art. 98 D.Lgs. 30 /2005 'Codice della Proprietà Industriale': 'Per segreti commerciali si intendono le informazioni aziendali e le esperienze tecnico-industriali, comprese quelle commerciali, soggette al legittimo controllo del detentore, ove tali informazioni: a) siano segrete, nel senso che non siano nel loro insieme o nella precisa configurazione e combinazione dei loro elementi generalmente note o facilmente accessibili agli esperti ed agli operatori del settore; b) abbiano valore economico in quanto segrete; c) siano sottoposte, da parte delle persone al cui legittimo controllo sono soggette, a misure da ritenersi ragionevolmente adeguate a mantenerle segrete.
2. Costituiscono altresì oggetto di protezione i dati relativi a prove o altri dati segreti, la cui elaborazione comporti un considerevole impegno ed alla cui presentazione sia subordinata l'autorizzazione dell'immissione in commercio di prodotti chimici, farmaceutici o agricoli implicanti l'uso di nuove sostanze chimiche').

Modello linguistico di grandi dimensioni (c.d. 'Large Language Model', LLM)
È una specie di 'modello di IA per finalità generali' (GPAI) ai sensi dell'art. 3(63) del Reg. (UE) 2024/1689 (AI Act) [23], specializzata nell'elaborazione e nella generazione di contenuti in linguaggio naturale.

Prompt
È un sottoinsieme di 'dati di input' ai sensi dell'art. 3(33) del Reg. (UE) 2024/1689 (AI Act), che consiste in un'istruzione o richiesta formulata in linguaggio naturale dall'utente e trasmessa a un modello linguistico di grandi dimensioni (LLM) al fine di ottenere un output.

Rischio
La combinazione dell'entità dell'impatto di un incidente, in termini di danno o di perturbazione, e della probabilità che quest'ultimo si verifichi (cfr. art. 2, lett. aa), D.Lgs. 138/2024);

Sistema di Intelligenza Artificiale
'Un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali', (cfr. art. 3(1) 'AI ACT', Comunicazione della Commissione Europea del 29 luglio 2025, C (2025) 5053 final) [24].

Note

22 Systemic Risks Associated with Agentic AI: A Policy Brief
↳ **Leggi**

23 Guidelines on the scope of obligations for providers of general-purpose AI models under the AI Act
↳ **Leggi**

24 Orientamenti della Commissione sulla definizione di sistema di intelligenza artificiale stabilita dal regolamento (UE) 2024/1689
↳ **Regolamento sull'IA**

8 Riconoscimenti

Hanno collaborato alla redazione del presente documento: Nicola Batzu, Ivan Codarin, Federico Costantini, Agostino Dovier, Pier Luca Montessoro, Francesco Pitassio, Fabio Romanelli, Giada Soncini, Mauro Volponi.