POLICY PER L'UTILIZZO DELL'INTELLIGENZA ARTIFICIALE IN CITTÀ METROPOLITANA DI GENOVA

Versione: 3.2
Data: 13 ottobre 2026

Tabella di Gestione del Documento

Vers	Data	Autore/i	Descrizione delle Modifiche	Stato	Approvato da
1.0	10/09/25	L. Papaleo (RTD)	Prima stesura della policy: definizione principi, governance iniziale e linee guida operative.	Superato	N/A
1.1	16/09/25	L. Papaleo (RTD)	Raffinamento contenuti su principi e linee guida operative AI Generativa.	superato	*N/A*
2.0	17/09/25	L. Papaleo (RTD), F. Rossi	Revisione: Integrazione fonti AgID e framework normativi. Istituzione del GL-IA e approccio basato sul rischio Dettaglio regole IA Generativa	Bozza da discutere con DG	*N/A*
3.0	23/01/26	L. Papaleo (RTD), M. Mordacci (DG)	Revisione: Aggiornamento sezione governance e correzioni minime su riferimenti e sezioni generali	Versione finale	Decreto Sindaco n. 18 del 26/02/2026
3.1	31/08/26	L. Papaleo (RTD)	Aggiornamento tecnico e normativo conseguente all'entrata in applicazione di ulteriori disposizioni, alle modifiche introdotte dal Regolamento (UE) 2026/1744 e agli orientamenti europei sulla trasparenza dei contenuti generati dall'IA. Razionalizzazione delle procedure di valutazione, acquisizione e utilizzo dei sistemi di IA.	Versione di lavoro	N/A
3.2	13/10/2026	L. Papaleo (RTD), M. Mordacci (DG)	Revisione: validazione dei contenuti proposti alla 3.1 e piccole correzioni chiarimenti per il ruolo di Responsabile del Sistema IA – aggiornamento del rinvio dinamico	Versione finale	Da approvare con Decreto della Sindaca Metropolitana.

SOMMARIO

Premessa e Finalità 3

Articolo I. Ambito di Applicazione 3

Articolo II. Principi Fondamentali 4

Articolo III. Governance e Ruoli 6

Articolo IV. Ciclo di Vita dei Sistemi di IA 8

Articolo V. Linee Guida per l'Uso dell'IA Generativa 10

Articolo VI. Formazione e Cultura dell'Innovazione 12

Articolo VII. Trasparenza, Informazione e Registrazione dei Sistemi di IA 12

Articolo VIII. Tutela della Proprietà Intellettuale 13

Articolo IX. Inosservanza della Policy 14

Articolo X. Riferimenti Normativi e Strategici 14

Articolo XI. REVISIONE E AGGIORNAMENTO DELLA POLICY 15

Allegato A Glossario 16

PREMESSA E FINALITÀ

La Città Metropolitana di Genova riconosce il potenziale dell'Intelligenza Artificiale (IA) come strumento strategico per migliorare l'efficienza dei servizi pubblici, ottimizzare i processi decisionali e promuovere lo sviluppo sostenibile del territorio.

Questa Policy ha l'obiettivo di definire un quadro di riferimento etico e operativo per l'introduzione e l'utilizzo di sistemi di IA all'interno dell'Ente, garantendo che ogni applicazione sia sviluppata e impiegata nel rispetto dei diritti fondamentali, dei principi di trasparenza, equità e responsabilità e del quadro normativo europeo e nazionale applicabile.

L'approccio dell'Ente è orientato alla sperimentazione responsabile e all'adozione graduale di soluzioni di IA, con una supervisione umana effettiva e un'attenzione prioritaria alla sicurezza dei dati e alla centralità della persona.

L'Ente opera, di norma, in qualità di soggetto che utilizza sistemi di IA sotto la propria autorità (deployer, secondo la terminologia del Regolamento (UE) 2024/1689), ferma restando la necessità di verificare, per ogni iniziativa, il ruolo effettivamente assunto lungo la catena del valore. Qualora l'Ente sviluppi direttamente un sistema, lo immetta in servizio con il proprio nome o marchio ovvero ne modifichi sostanzialmente la finalità o il funzionamento, sono valutati anche gli eventuali obblighi applicabili al fornitore.

La presente Policy è coordinata con gli strumenti di programmazione dell'Ente (DUP, PIAO, Piano Strategico e Piano Triennale ICT, quando adottato) e ne costituisce riferimento operativo per la pianificazione, l'acquisizione e la gestione dei sistemi di IA.

La Policy è attuata secondo criteri di proporzionalità e sostenibilità organizzativa, differenziando gli adempimenti in relazione alla finalità, al contesto di utilizzo, ai dati trattati, ai soggetti interessati e al livello di rischio del sistema.

Articolo I. AMBITO DI APPLICAZIONE

La presente Policy si applica alle iniziative di progettazione, sviluppo, acquisizione, configurazione, sperimentazione, messa in servizio, utilizzo, monitoraggio e dismissione dei sistemi di IA impiegati dall'Ente, secondo modalità proporzionate alla natura, alla finalità e al livello di rischio del sistema o del caso d'uso.

La qualificazione di una soluzione come sistema di IA è effettuata sulla base della definizione contenuta nel Regolamento (UE) 2024/1689 e dei relativi orientamenti applicativi. Non rientrano automaticamente nell'ambito della presente Policy tutti i sistemi informatici basati su regole deterministiche, le automazioni procedurali tradizionali o le funzionalità statistiche prive delle caratteristiche proprie di un sistema di IA.

La Policy è vincolante per tutto il personale dipendente, i dirigenti e i collaboratori esterni che, a qualsiasi titolo, partecipano all'adozione, alla configurazione o all'utilizzo dei sistemi di IA.

La Policy si applica, per quanto pertinente e attraverso specifiche clausole contrattuali o convenzionali, anche ai fornitori e ai partner che progettano, sviluppano, forniscono, configurano o

gestiscono sistemi di IA per conto dell'Ente. Gli obblighi richiesti a tali soggetti sono determinati tenendo conto del ruolo assunto nella catena del valore, del livello di rischio, delle caratteristiche del servizio e della disciplina applicabile.

Articolo II. PRINCIPI FONDAMENTALI

Ogni iniziativa legata all'IA deve attenersi ai seguenti principi:

(1) ANTROPOCENTRISMO, CONTROLLO E SUPERVISIONE UMANA: i sistemi di IA sono utilizzati come strumenti di supporto all'attività dell'Ente e non sostituiscono le competenze, le responsabilità e il potere valutativo attribuiti alle persone dalla normativa e dall'organizzazione amministrativa. La supervisione umana è effettiva e proporzionata alla finalità, al livello di autonomia e ai rischi del sistema. Nei casi più rilevanti sono individuati soggetti dotati di adeguate competenze, formazione, autorità e possibilità concreta di comprendere, verificare, non utilizzare, correggere o interrompere il funzionamento del sistema. Nessuna decisione con effetti giuridici o analogamente significativi sulle persone può essere adottata esclusivamente sulla base dell'output di un sistema di IA.

(2) EQUITÀ E NON DISCRIMINAZIONE: l'Ente si impegna a prevenire e mitigare la creazione o l'amplificazione di distorsioni discriminatorie. Quando i dati utilizzati o forniti dall'Ente possono incidere sul funzionamento o sugli output del sistema, ne sono valutate, in misura proporzionata al caso d'uso, la pertinenza, la qualità, l'adeguatezza, la provenienza e le eventuali distorsioni.

(3) TRASPARENZA, COMPRENSIBILITÀ E SPIEGABILITÀ: l'impiego dei sistemi di IA deve essere documentato e reso comprensibile in misura adeguata alla finalità, ai destinatari e agli effetti prodotti. Nei processi che incidono su diritti o interessi delle persone devono essere disponibili informazioni utili a comprendere il ruolo svolto dal sistema, i principali fattori rilevanti, i suoi limiti e le modalità di supervisione e riesame umano. Restano fermi, nei rispettivi ambiti di applicazione, i diritti e gli obblighi previsti dal GDPR, dal Regolamento (UE) 2024/1689 e dalla normativa sul procedimento amministrativo.

(4) PROTEZIONE DEI DATI E SICUREZZA FIN DALLA PROGETTAZIONE E PER IMPOSTAZIONE PREDEFINITA: ogni soluzione di IA deve essere valutata nel rispetto della normativa sulla protezione dei dati personali, della sicurezza informatica, della continuità operativa e della classificazione dei dati e dei servizi dell'Ente. Il trattamento è limitato ai dati necessari rispetto alla finalità autorizzata e deve avvenire mediante strumenti, configurazioni e modalità coerenti con il livello di rischio.

(5) RESPONSABILITÀ E RENDICONTAZIONE (ACCOUNTABILITY): per ciascun sistema o insieme omogeneo di casi d'uso deve essere chiaramente individuato un punto di riferimento amministrativo per il relativo contesto di utilizzo, ferme restando le responsabilità attribuite dalla legge, dall'ordinamento dell'Ente e dal contratto agli altri soggetti coinvolti.

(6) SOSTENIBILITÀ: l'utilizzo degli strumenti di IA deve tenere conto del loro impatto ambientale e sociale. L'Ente promuove un approccio consapevole che ottimizzi l'uso delle risorse computazionali, privilegiando, ove possibile, soluzioni a minore consumo energetico.

(7) PROPORZIONALITÀ E MINIMIZZAZIONE DEL RISCHIO: la complessità delle soluzioni di IA e degli adempimenti di controllo deve essere proporzionata alla finalità pubblica perseguita, al contesto di utilizzo e ai rischi effettivi. A parità di risultato sono privilegiate soluzioni meno intrusive, più sicure e maggiormente comprensibili.

(8) AUDITABILITÀ, DOCUMENTAZIONE E TRACCIABILITÀ: per ciascun sistema o caso d'uso sono individuate, in misura proporzionata al rischio, le informazioni, le evidenze e gli eventuali log necessari a documentarne l'approvazione, l'utilizzo, la supervisione e il monitoraggio. I tempi di conservazione sono definiti tenendo conto della finalità, della normativa archivistica, della protezione dei dati personali, degli obblighi dell'AI Act e delle esigenze di sicurezza.

(9) CONTESTABILITÀ: ogni decisione o valutazione individuale nella quale l'output di un sistema di IA abbia assunto un ruolo sostanziale deve poter essere compresa, riesaminata e, se necessario, corretta da un operatore umano. Le persone interessate devono poter ottenere informazioni comprensibili sul ruolo del sistema, chiedere il riesame umano e, nei casi previsti, contestare l'esito attraverso i rimedi amministrativi o giurisdizionali applicabili.

Pratiche vietate

È vietata la proposta, l'acquisizione, la sperimentazione o l'utilizzo da parte dell'Ente di sistemi di IA rientranti nelle pratiche vietate dall'articolo 5 del Regolamento (UE) 2024/1689 e successive modificazioni. Sono in particolare vietati, salvo le specifiche eccezioni previste dalla normativa:

- sistemi che impiegano tecniche manipolative, ingannevoli o subliminali idonee a compromettere la capacità delle persone di assumere decisioni consapevoli e a causare un danno significativo;
- sistemi che sfruttano vulnerabilità connesse all'età, alla disabilità o a particolari condizioni sociali o economiche;
- sistemi di valutazione o classificazione sociale delle persone basati sul comportamento o su caratteristiche personali, quando producano trattamenti sfavorevoli ingiustificati o sproporzionati;
- sistemi diretti a prevedere il rischio che una persona commetta un reato esclusivamente sulla base della profilazione o della valutazione di caratteristiche personali;
- sistemi che creano o ampliano banche dati per il riconoscimento facciale attraverso la raccolta indiscriminata di immagini da Internet o da sistemi di videosorveglianza;
- sistemi di riconoscimento delle emozioni nei luoghi di lavoro, salvo i casi espressamente ammessi per motivi medici o di sicurezza;
- sistemi di categorizzazione biometrica diretti a dedurre caratteristiche personali sensibili;
- sistemi di identificazione biometrica remota in tempo reale negli spazi accessibili al pubblico, salvo i casi e le garanzie espressamente previsti dalla legge;
- ulteriori pratiche vietate dalla normativa europea o nazionale vigente.

La verifica dell'eventuale riconducibilità del sistema a una pratica vietata costituisce il primo passaggio della valutazione preliminare prevista dall'articolo IV.

Articolo III. GOVERNANCE E RUOLI

Assetto di governance dell'Intelligenza Artificiale: la governance dei sistemi di IA della Città Metropolitana di Genova è affidata a un presidio centrale unitario, finalizzato a garantire responsabilità, coerenza strategica e conformità normativa nell'adozione e nell'uso dell'IA.

La governance è esercitata congiuntamente dal Direttore Generale e Segretario Generale e dal Responsabile per la Transizione Digitale (RTD), con il supporto dell'Ufficio per la Transizione Digitale (UTD). Il presidio centrale di governance:

- assicura la coerenza dell'uso dell'IA con gli strumenti di programmazione dell'Ente (DUP, PIAO, Piano Strategico e Piano Triennale ICT, quando adottato);
- garantisce il rispetto del quadro normativo vigente e degli indirizzi nazionali ed europei applicabili;
- supervisiona l'attuazione della presente Policy lungo l'intero ciclo di vita dei sistemi di IA;
- opera secondo criteri di proporzionalità, evitando duplicazioni rispetto ai procedimenti, alle valutazioni e ai sistemi di controllo già previsti dalla normativa e dall'organizzazione dell'Ente.

RUOLO DEL RTD E DELL'UFFICIO PER LA TRANSIZIONE DIGITALE: il RTD, avvalendosi dell'UTD:

- coordina operativamente l'attuazione della presente Policy;
- supporta le Direzioni e i Servizi nella progettazione, acquisizione, utilizzo e dismissione dei sistemi di IA;
- cura l'istituzione e il coordinamento del Registro interno dei sistemi e dei casi d'uso di IA, nonché la pubblicazione delle informazioni destinate al Registro pubblico, sulla base dei contenuti forniti e validati dai Dirigenti e dai Responsabili dei sistemi interessati;
- definisce, aggiorna e rende disponibili modelli proporzionati di screening, valutazione, registrazione e monitoraggio dei sistemi e dei casi d'uso;
- promuove l'adozione di standard, modelli e checklist di conformità, in coerenza con l'approccio basato sul rischio;
- assicura il raccordo con i profili di sicurezza informatica, architettura ICT, interoperabilità e continuità operativa;
- coordina il monitoraggio degli aggiornamenti normativi, delle Linee guida e degli standard tecnici applicabili, proponendo gli adeguamenti della Policy e delle relative istruzioni operative.

COLLABORAZIONI OPERATIVE E COMPETENZE SPECIALISTICHE: per ciascun sistema di IA o caso d'uso, il presidio centrale di governance attiva collaborazioni operative mirate, in funzione delle caratteristiche del sistema, della finalità perseguita e dei rischi connessi. Sono coinvolti, ove pertinenti:

- il Responsabile della Protezione dei Dati (DPO), nei casi in cui il sistema comporti trattamenti di dati personali che richiedano valutazioni specialistiche, presenti un rischio potenzialmente elevato per i diritti e le libertà delle persone o renda necessaria una valutazione d'impatto sulla protezione dei dati. Il DPO è consultato e svolge le proprie funzioni in autonomia, senza assumere responsabilità gestionali o decisionali sul sistema;

- il RUP e le strutture competenti in materia di contratti pubblici, secondo la ripartizione delle competenze prevista dall'organizzazione dell'Ente;
- le strutture ICT competenti, per gli aspetti di sicurezza, architettura, integrazione e continuità operativa.

Possono inoltre essere coinvolti, in relazione allo specifico ambito di applicazione, i Direttori delle Direzioni tecniche, il Responsabile delle Risorse Umane, le strutture competenti in materia di trasparenza, anticorruzione e controlli interni, nonché ulteriori competenze specialistiche. Le collaborazioni hanno natura operativa e contestualizzata e non comportano l'istituzione di ulteriori organismi permanenti.

RESPONSABILE DEL SISTEMA IA: per ciascun sistema di IA adottato dall'Ente o per un insieme omogeneo di casi d'uso riconducibili al medesimo servizio può essere individuato un Responsabile del Sistema IA, quale punto di riferimento – con il supporto del RTD – per il relativo contesto di utilizzo. Il Responsabile coincide, di norma:

- con il Direttore o Dirigente responsabile del settore o del servizio nell'ambito del quale il sistema è utilizzato;
- con il Direttore Generale, nei casi in cui il sistema abbia carattere trasversale, incida su più strutture organizzative o supporti funzioni di coordinamento generale dell'Ente.

Il Responsabile del Sistema IA:

- garantisce che il sistema sia utilizzato esclusivamente per le finalità istituzionali autorizzate;
- assicura l'attuazione delle misure di supervisione umana, trasparenza, proporzionalità e non discriminazione pertinenti al caso d'uso;
- vigila sull'attuazione delle misure di mitigazione dei rischi definite in sede di istruttoria;
- collabora con RTD e UTD per il monitoraggio, la gestione degli incidenti e l'aggiornamento dei registri;
- garantisce, ove applicabile, la possibilità di contestazione e riesame delle decisioni assistite dall'IA.

Il Responsabile del Sistema IA non assume le responsabilità proprie del fornitore, del titolare del trattamento, del RUP, del responsabile del procedimento, del dirigente competente o delle strutture tecniche e di sicurezza.

RESPONSABILITÀ DEI DIRETTORI E DEI DIRIGENTI: i Direttori e i Dirigenti restano responsabili dei procedimenti e dei servizi di competenza nei quali sono utilizzati sistemi di IA e garantiscono:

- la corretta istruttoria delle proposte di adozione o utilizzo dei sistemi;
- la collaborazione con il presidio di governance, il RTD e l'UTD;
- l'applicazione delle misure di supervisione umana e di mitigazione dei rischi;
- le attività di monitoraggio e segnalazione previste dalla presente Policy.

Articolo IV. Ciclo di Vita dei Sistemi di IA

FASE 1 - Progettazione, valutazione preliminare e acquisizione

Prima dell'avvio di un progetto, di una sperimentazione o dell'acquisizione di una soluzione di IA, la struttura proponente effettua una valutazione preliminare proporzionata, con il supporto del RTD e con il coinvolgimento del DPO nei casi di competenza, volta a:

- verificare che la soluzione rientri nella definizione di sistema di IA;
- individuare il caso d'uso, la finalità istituzionale, i benefici attesi e le eventuali alternative meno rischiose;
- identificare il ruolo assunto dall'Ente nella catena del valore;
- escludere la riconducibilità del sistema alle pratiche vietate;
- classificare il sistema e il caso d'uso secondo l'AI Act e il modello interno adottato dall'Ente;
- individuare i dati trattati, le fonti, i flussi informativi e gli eventuali trattamenti di dati personali;
- valutare gli impatti sui diritti fondamentali, sulla trasparenza, sulla non discriminazione, sulla sicurezza, sull'organizzazione e sulla continuità del servizio;
- definire le misure di supervisione umana, monitoraggio, mitigazione dei rischi e gestione degli incidenti;
- verificare gli obblighi di informazione, registrazione e trasparenza applicabili;
- individuare il Responsabile del Sistema IA, ove necessario.

La valutazione può concludersi con:

- autorizzazione semplificata per casi d'uso a basso rischio;
- autorizzazione accompagnata da specifiche misure di mitigazione;
- necessità di ulteriori approfondimenti, inclusa la valutazione d'impatto sui diritti fondamentali (FRIA/VIA) o la DPIA;
- non autorizzazione del sistema o del caso d'uso.

Per i sistemi ad alto rischio ai quali si applica l'articolo 27 del Regolamento (UE) 2024/1689, la valutazione preliminare è integrata dalla valutazione d'impatto sui diritti fondamentali. Quando il sistema comporta trattamenti suscettibili di presentare un rischio elevato per i diritti e le libertà delle persone, è inoltre effettuata la DPIA prevista dal GDPR.

(a) Documentazione richiesta ai fornitori

La documentazione richiesta al fornitore è determinata in modo proporzionato al livello di rischio, al ruolo assunto dall'Ente e alle caratteristiche della soluzione. Può comprendere, ove pertinente:

- descrizione del sistema, finalità prevista, funzionalità di IA e limiti d'uso;
- classificazione ai sensi dell'AI Act e ruolo dei soggetti coinvolti;
- istruzioni d'uso e misure di supervisione umana;
- informazioni sulle prestazioni, sull'accuratezza, sulla robustezza e sui limiti conosciuti;

- documentazione tecnica, Model Card o documentazione equivalente, se disponibile e pertinente;
- informazioni sui dati utilizzati e sulla relativa provenienza, quando rilevanti e accessibili;
- modalità di conservazione e utilizzo dei dati, inclusa l'esclusione o la disciplina dell'addestramento sui dati dell'Ente;
- localizzazione dei dati, trasferimenti internazionali e subfornitori;
- misure di sicurezza, gestione delle vulnerabilità e degli incidenti;
- logging, controllo degli accessi e conservazione delle evidenze;
- gestione degli aggiornamenti e delle modifiche del modello;
- condizioni di portabilità, restituzione e cancellazione dei dati;
- disciplina della proprietà intellettuale e dei diritti sugli output;
- piano di continuità, cessazione e dismissione del servizio.

Per i sistemi ad alto rischio devono essere acquisite le informazioni e le evidenze previste dal Regolamento (UE) 2024/1689. Per servizi standard o a basso rischio, la documentazione può essere semplificata e basata sulle informazioni ragionevolmente disponibili sul mercato.

(b) SERVIZI CLOUD E SICUREZZA

L'acquisizione di servizi di IA erogati in modalità cloud avviene nel rispetto della disciplina nazionale sulla qualificazione dei servizi cloud per la Pubblica Amministrazione, della classificazione dei dati e dei servizi e delle disposizioni dell'Agenzia per la cybersicurezza nazionale. Quando la qualificazione è obbligatoria, essa costituisce requisito necessario e non può essere sostituita da una generica dichiarazione di equivalenza. Devono inoltre essere valutate la localizzazione e i trasferimenti dei dati, la continuità operativa, la gestione degli accessi, la sicurezza della catena di fornitura e le modalità di cessazione del servizio.

FASE 2 - SVILUPPO, SPERIMENTAZIONE E VALIDAZIONE

Ogni sistema deve essere verificato, prima della messa in esercizio, mediante modalità proporzionate alla natura e al rischio. Per i sistemi sviluppati o configurati dall'Ente sono effettuati test in ambiente controllato sull'affidabilità, la robustezza, la sicurezza e le eventuali distorsioni discriminatorie.

Per i sistemi acquisiti come servizio standard, la validazione può essere effettuata attraverso una sperimentazione controllata su casi d'uso rappresentativi, senza impiego di dati non autorizzati, verificando qualità degli output, limiti, affidabilità, sicurezza e adeguatezza delle misure di supervisione.

È utilizzata, secondo criteri di proporzionalità, una checklist preliminare alla messa in esercizio che può includere: esito della classificazione; VIA/FRIA o DPIA ove dovute; test di robustezza e non discriminazione; piano di supervisione umana; configurazione del logging; piano di monitoraggio e dismissione; verifiche tecniche e di sicurezza, inclusi test di vulnerabilità o penetration test ove giustificati dalla criticità e dall'architettura del sistema.

FASE 3 - MONITORAGGIO, INCIDENTI E DISMISSIONE

I sistemi in esercizio sono sottoposti a monitoraggio proporzionato per verificarne nel tempo l'adeguatezza, il corretto funzionamento e il rispetto delle condizioni autorizzate. Ove pertinente, sono definiti indicatori, soglie di allerta e modalità di riesame.

Il monitoraggio tiene conto anche delle modifiche rilevanti delle funzionalità, del modello, delle condizioni contrattuali, dei subfornitori o delle modalità di trattamento dei dati. Tali modifiche possono determinare la necessità di aggiornare la valutazione preliminare.

In caso di evento avverso, anomalia o superamento delle soglie è attivata la procedura di segnalazione al Responsabile del Sistema IA, al RTD e alle strutture tecniche competenti, ferme restando le procedure previste per gli incidenti di sicurezza, i data breach, la continuità operativa e le eventuali comunicazioni alle autorità o al fornitore.

La dismissione è pianificata e gestita in sicurezza, prevedendo, ove applicabile, restituzione, portabilità, cancellazione o anonimizzazione dei dati, revoca degli accessi, conservazione delle evidenze necessarie e aggiornamento dei registri.

Articolo V. LINEE GUIDA PER L'USO DELL'IA GENERATIVA

L'uso di strumenti di IA generativa per finalità istituzionali è consentito esclusivamente nel rispetto della presente Policy, delle istruzioni operative dell'Ente e delle limitazioni associate allo specifico strumento o caso d'uso.

Gli strumenti sono distinti in:

- strumenti non autorizzati o utilizzati attraverso account personali;
- strumenti autorizzati dall'Ente per attività istituzionali a basso rischio;
- sistemi autorizzati per specifici casi d'uso, dati o processi.

Negli strumenti non autorizzati o utilizzati attraverso account personali possono essere inserite esclusivamente informazioni già pubbliche, prive di informazioni riservate, segreti d'ufficio o contenuti la cui trasmissione a soggetti terzi non sia autorizzata.

Negli strumenti istituzionali autorizzati possono essere trattati esclusivamente i dati, i documenti e i casi d'uso ammessi dalle relative istruzioni operative, nel rispetto delle misure tecniche, organizzative, contrattuali e di protezione dei dati definite dall'Ente. L'autorizzazione di uno strumento non implica l'autorizzazione indiscriminata di qualsiasi utilizzo o categoria di dati.

VERIFICA DEGLI OUTPUT E RESPONSABILITÀ

Gli output generati dall'IA costituiscono contenuti di supporto e non “documenti finali”. Prima del loro utilizzo devono essere verificati in relazione all'accuratezza, alla completezza, alla pertinenza, all'aggiornamento, alla coerenza con le fonti e all'assenza di contenuti discriminatori, illeciti o lesivi dei diritti di terzi.

L'utilizzatore deve apportare le modifiche necessarie e assicurare che il contenuto finale sia adeguato alla finalità amministrativa e al destinatario. La responsabilità del procedimento,

dell'istruttoria, della valutazione e della sottoscrizione resta attribuita ai soggetti individuati dalla normativa e dall'organizzazione dell'Ente.

ATTI E DOCUMENTI AMMINISTRATIVI

L'IA generativa può essere utilizzata per attività preparatorie, redazionali o di revisione di atti e documenti amministrativi, purché non sostituisca l'istruttoria, la valutazione giuridico-amministrativa, la motivazione e l'assunzione di responsabilità da parte dei soggetti competenti. Non è consentito recepire un output senza averne verificato puntualmente contenuto, fonti, presupposti, riferimenti normativi e coerenza con gli atti del procedimento.

INTERAZIONE CON CITTADINI E ALTRI UTENTI

Quando un sistema di IA interagisce direttamente con cittadini o altri utenti, questi sono informati in modo chiaro, tempestivo e accessibile della natura artificiale dell'interlocutore, salvo che ciò risulti già evidente nelle circostanze concrete. Nei servizi istituzionali devono inoltre essere definiti:

- finalità e limiti del servizio;
- modalità per richiedere l'intervento o il riesame umano;
- trattamento e tempi di conservazione delle conversazioni;
- misure contro contenuti illeciti, inappropriati o fuorvianti;
- accessibilità del servizio;
- gestione degli errori, delle segnalazioni e degli incidenti.

TRASPARENZA DEI CONTENUTI

Le immagini, gli audio e i video artificialmente generati o manipolati che possano apparire autentici sono accompagnati, nei casi previsti dall'articolo 50 del Regolamento (UE) 2024/1689, da un'indicazione chiara e accessibile della loro natura artificiale.

I testi generati o manipolati dall'IA e pubblicati per informare il pubblico su questioni di interesse pubblico sono sottoposti a un effettivo processo di revisione e controllo editoriale umano, con individuazione della persona o struttura responsabile della pubblicazione. Quando tale controllo non ricorre, il contenuto deve essere identificato come generato o manipolato dall'IA secondo la normativa applicabile.

Le eventuali modalità di etichettatura sono definite con istruzioni operative del RTD, tenendo conto delle Linee guida e degli strumenti adottati a livello europeo.

USI VIETATI

Sono vietati la generazione o diffusione di contenuti intenzionalmente fuorvianti o manipolativi, la simulazione illecita di identità, l'elusione di norme o procedure, l'adozione automatica di atti o decisioni e ogni utilizzo contrario alle pratiche vietate o alle limitazioni definite dall'Ente.

DOVERI DELL'UTILIZZATORE

Ogni utilizzatore è tenuto a rispettare la presente Policy, le istruzioni operative e le limitazioni associate allo strumento, a verificare gli output prima del loro impiego e a segnalare tempestivamente anomalie, utilizzi impropri o incidenti. Restano ferme le responsabilità attribuite dalla normativa e dall'organizzazione dell'Ente ai dirigenti, ai responsabili dei procedimenti, al RUP, ai Responsabili dei sistemi e agli altri soggetti coinvolti.

Articolo VI. FORMAZIONE E CULTURA DELL'INNOVAZIONE

La Città Metropolitana di Genova promuove un programma di formazione continua per diffondere tra il personale le competenze necessarie a comprendere e utilizzare consapevolmente gli strumenti di IA, riconoscendone opportunità, limiti e rischi. La partecipazione alle iniziative formative individuate dall'Ente costituisce un dovere per il personale interessato.

La formazione costituisce una delle misure adottate dall'Ente per sostenere lo sviluppo dell'alfabetizzazione in materia di IA ai sensi dell'articolo 4 del Regolamento (UE) 2024/1689, come modificato dal Regolamento (UE) 2026/1744, ed è definita tenendo conto delle conoscenze tecniche, dell'esperienza, del ruolo del personale, dei sistemi utilizzati e dei rischi per le persone potenzialmente interessate.

La formazione è organizzata su tre livelli: (1) base per tutto il personale, sui fondamenti dell'IA, sui rischi e sulle regole per l'IA generativa; (2) avanzata per dirigenti, RUP e responsabili di procedimento, sulla governance del rischio, sulle responsabilità e sul procurement; (3) specialistica per RTD, UTD, strutture ICT, cybersecurity e DPO, sugli aspetti tecnici, di sicurezza, valutazione d'impatto e spiegabilità.

Le iniziative formative sono documentate attraverso programmi, materiali, destinatari e partecipazione. L'accesso a determinati sistemi o casi d'uso può essere subordinato al completamento della formazione individuata come necessaria. I contenuti sono riesaminati periodicamente e aggiornati quando intervengano modifiche normative, tecnologiche o organizzative rilevanti.

Articolo VII. TRASPARENZA, INFORMAZIONE E REGISTRAZIONE DEI SISTEMI DI IA

L'Ente istituisce un Registro interno dei sistemi e dei casi d'uso di IA autorizzati, coordinato dal RTD e alimentato dai Dirigenti e dai Responsabili dei sistemi interessati.

Il Registro interno contiene, in misura proporzionata:

- denominazione e descrizione del sistema;
- finalità e struttura utilizzatrice;
- fornitore e ruolo dell'Ente;
- casi d'uso autorizzati;
- livello di rischio e data della valutazione;
- dati o categorie di dati ammessi;

- Responsabile del Sistema IA, ove individuato;
- misure di supervisione umana;
- principali limitazioni e misure di mitigazione;
- stato del sistema e date di avvio, riesame e dismissione.

L'Ente pubblica sul proprio sito istituzionale le informazioni relative ai sistemi di IA che interagiscono con il pubblico, incidono sui servizi ai cittadini o presentano un impatto significativo sui diritti e sugli interessi delle persone.

Il Registro pubblico indica, in forma chiara e accessibile:

- finalità e ambito di utilizzo;
- ruolo svolto dal sistema;
- struttura responsabile;
- presenza e modalità della supervisione umana;
- principali capacità e limitazioni;
- modalità per richiedere informazioni, segnalare problemi o ottenere il riesame umano;
- ulteriori informazioni previste dalla normativa.

Sono fatti salvi i limiti derivanti dalla protezione dei dati personali, dalla sicurezza informatica, dai segreti tutelati dalla legge e dai diritti di proprietà intellettuale. Le informazioni sono aggiornate quando intervengono modifiche rilevanti e comunque sottoposte a verifica periodica.

Restano fermi gli eventuali obblighi di registrazione nella banca dati europea dei sistemi ad alto rischio.

Articolo VIII. TUTELA DELLA PROPRIETÀ INTELLETTUALE

L'utilizzo di dati, documenti, immagini, testi, software e altri contenuti nei sistemi di IA deve rispettare i diritti d'autore, le licenze, i diritti sulle banche dati, gli obblighi di riservatezza e le condizioni d'uso applicabili.

Non possono essere utilizzati come input contenuti protetti quando l'Ente non disponga di un titolo, di una licenza, di un'autorizzazione o di altra base giuridica che ne consenta l'utilizzo. Prima della diffusione esterna degli output devono essere valutati, in misura proporzionata, l'eventuale riproduzione di contenuti di terzi, il rischio di plagio e le condizioni contrattuali relative ai diritti di utilizzazione.

I contratti disciplinano, in misura adeguata alla tipologia e al valore dell'affidamento, i diritti di utilizzo degli input e degli output, le garanzie sulla legittima disponibilità dei modelli e dei dati, le responsabilità per pretese di terzi e l'assistenza del fornitore in caso di contestazioni. L'eventuale previsione di garanzie o manleve è valutata in relazione al rischio e alle condizioni effettivamente disponibili sul mercato.

Articolo IX. Inosservanza della Policy

La violazione della presente Policy e delle relative istruzioni operative è valutata secondo la normativa vigente, i contratti collettivi, il Codice di comportamento e i regolamenti dell'Ente, tenendo conto della gravità della condotta, dell'elemento soggettivo, del ruolo ricoperto, della formazione ricevuta, del danno o rischio prodotto e delle misure adottate per prevenirlo o limitarlo.

Restano ferme le eventuali responsabilità civili, penali, amministrative, contabili o disciplinari previste dall'ordinamento.

L'Ente promuove la tempestiva segnalazione, anche in buona fede, di errori, anomalie, vulnerabilità, incidenti o utilizzi impropri dei sistemi di IA. Le segnalazioni sono gestite attraverso i canali appropriati, inclusi, quando ne ricorrano i presupposti, quelli previsti dalla disciplina sul whistleblowing.

Articolo X. Riferimenti Normativi e Strategici

La presente Policy è redatta in coerenza con i principali quadri di riferimento europei e nazionali in materia di intelligenza artificiale, innovazione digitale, organizzazione amministrativa, contratti pubblici, sicurezza e protezione dei dati personali. I riferimenti si intendono effettuati ai testi vigenti e alle successive modificazioni. In particolare:

- Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, che stabilisce regole armonizzate sull'intelligenza artificiale (AI Act).
  Testo ufficiale: https://eur-lex.europa.eu/eli/reg/2024/1689/oj?locale=it
- Regolamento (UE) 2026/1744, recante modifiche e semplificazioni nell'attuazione delle regole armonizzate sull'intelligenza artificiale.
  Testo ufficiale: https://eur-lex.europa.eu/eli/reg/2026/1744/oj
- Regolamento (UE) 2016/679 (GDPR) e Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i., in materia di protezione dei dati personali.
- Legge 23 settembre 2025, n. 132, recante disposizioni e deleghe al Governo in materia di intelligenza artificiale.
- Decreto Legislativo 7 marzo 2005, n. 82 e s.m.i. - Codice dell'Amministrazione Digitale.
- Legge 7 agosto 1990, n. 241 e Decreto Legislativo 14 marzo 2013, n. 33, per i profili relativi al procedimento, alla motivazione, alla trasparenza e all'accesso.
- Decreto Legislativo 31 marzo 2023, n. 36 e s.m.i. - Codice dei contratti pubblici.
- Decreto Legislativo 4 settembre 2024, n. 138, di recepimento della direttiva NIS2, per il coordinamento con la gestione del rischio e degli incidenti di cybersicurezza.
- Decreto Legislativo 18 agosto 2000, n. 267 e s.m.i. - Testo Unico delle Leggi sull'Ordinamento degli Enti Locali.
- Piano Integrato di Attività e Organizzazione (PIAO) e strumenti di programmazione dell'Ente.
- Linee guida e documenti di indirizzo adottati o posti in consultazione da AgID in materia di adozione, sviluppo e procurement dei sistemi di IA nella Pubblica Amministrazione, nei rispettivi stati di efficacia.

- Linee guida della Commissione europea sugli obblighi di trasparenza dell'articolo 50 dell'AI Act e Codice di buone pratiche sulla trasparenza dei contenuti generati dall'IA.
- Strategia Italiana per l'Intelligenza Artificiale 2024-2026 e relativi aggiornamenti.
- Orientamenti etici per un'Intelligenza Artificiale affidabile della Commissione europea e Principi OCSE sull'Intelligenza Artificiale.

Articolo XI. REVISIONE E AGGIORNAMENTO DELLA POLICY

La presente Policy è soggetta a riesame periodico e, in ogni caso, qualora intervengano modifiche normative, tecnologiche o organizzative rilevanti.

Ogni richiamo a disposizioni legislative o regolamentari contenuto nella presente Policy si intende riferito al testo vigente e alle sue successive modificazioni e integrazioni. Le disposizioni normative sopravvenute prevalgono sulle eventuali previsioni incompatibili della Policy, senza determinare una modifica testuale automatica del documento. Il RTD cura il monitoraggio del quadro normativo e propone gli aggiornamenti necessari secondo le modalità indicate nel presente articolo. Gli atti di indirizzo, le linee guida e gli standard tecnici trovano applicazione nei limiti della loro efficacia giuridica e del relativo ambito di applicazione.

Gli aggiornamenti ordinari, tecnici, procedurali o di mero allineamento e coordinamento formale con la normativa sovraordinata tempo per tempo vigente — che rivestano carattere non sostanziale — sono approvati con atto del Direttore Generale, su proposta del RTD, ai sensi del relativo Decreto del Sindaco Metropolitano.

Le modifiche sostanziali incidenti sui principi fondamentali, sull'assetto di governance o sugli indirizzi generali rimangono riservate alla competenza del Sindaco Metropolitano e sono approvate con le medesime modalità previste per l'adozione iniziale.

Le istruzioni operative, i modelli, le checklist, i registri tecnici e gli altri allegati applicativi che non incidono sui principi, sulla governance o sugli indirizzi generali possono essere adottati, modificati e aggiornati direttamente con provvedimento del RTD, informandone il Direttore Generale e le strutture interessate.

Per ogni aggiornamento, a prescindere dall'organo che lo ha approvato, è mantenuto a cura del RTD un registro delle versioni recante data, estremi dell'atto di approvazione e sintesi delle modifiche apportate.

ALLEGATO A GLOSSARIO

Di seguito sono riportate le definizioni dei principali termini utilizzati nella presente Policy, al fine di garantirne una comprensione uniforme.

Algoritmo: sequenza finita di istruzioni o regole logico-matematiche eseguita da un sistema informatico per risolvere un problema o svolgere un compito specifico.

Anonimizzazione: processo che modifica i dati personali in modo irreversibile, così da rendere non identificabile la persona cui si riferiscono, tenendo conto dei mezzi ragionevolmente utilizzabili.

Bias o distorsione: tendenza sistematica di un sistema o dei suoi output a produrre risultati inesatti, squilibrati o ingiustamente sfavorevoli per determinate persone o gruppi.

Caso d'uso: specifica modalità con la quale un sistema di IA viene impiegato in un determinato processo, contesto organizzativo e per una finalità definita.

Ciclo di vita dell'IA: insieme delle fasi relative a un sistema, dall'ideazione e progettazione, allo sviluppo o acquisizione, validazione, messa in esercizio, monitoraggio e dismissione.

Contenuto sintetico: contenuto audio, visivo, video o testuale generato o manipolato mediante un sistema di IA.

Dati appartenenti a categorie particolari: dati personali di cui all'articolo 9 del GDPR. La relativa nozione non coincide con la più generica espressione 'dati sensibili'.

Deepfake: contenuto generato o manipolato dall'IA, costituito da immagini, audio o video, che assomiglia a persone, oggetti, luoghi, entità o eventi esistenti e che apparirebbe falsamente autentico o veritiero a una persona.

Deployer: persona fisica o giuridica, autorità pubblica, agenzia o altro organismo che utilizza un sistema di IA sotto la propria autorità, salvo gli usi personali non professionali.

DPIA: valutazione d'impatto sulla protezione dei dati ai sensi dell'articolo 35 del GDPR.

FRIA/VIA: valutazione d'impatto sui diritti fondamentali prevista, per i casi applicabili, dall'articolo 27 dell'AI Act. Nella presente Policy l'espressione VIA indica anche il modello interno di valutazione degli impatti algoritmici, utilizzabile in forma proporzionata per ulteriori casi d'uso.

Human-in-the-Loop o supervisione umana: insieme di misure organizzative e tecniche che consentono a persone dotate di competenza, formazione e autorità adeguate di comprendere, sorvegliare, verificare, non utilizzare, correggere o interrompere il funzionamento o gli output di un sistema, in misura proporzionata ai rischi.

Incident Reporting IA: procedura di segnalazione e gestione di eventi avversi, anomalie, malfunzionamenti o utilizzi impropri connessi ai sistemi di IA.

Intelligenza Artificiale generativa (IAG): sistemi o modelli capaci di generare nuovi contenuti, quali testi, immagini, audio, video o codice, a partire dagli input ricevuti.

Model Card o documentazione equivalente: documentazione sintetica relativa a finalità, caratteristiche, prestazioni, limiti e condizioni d'uso di un modello o sistema di IA.

Modello di IA per finalità generali (GPAI): modello di IA che presenta una generalità significativa, è in grado di svolgere con competenza un'ampia gamma di compiti distinti ed è integrabile in molteplici sistemi o applicazioni a valle.

Modifica sostanziale: cambiamento apportato a un sistema dopo la sua immissione sul mercato o messa in servizio, non previsto nella valutazione iniziale e idoneo a incidere sulla conformità o a modificare la finalità prevista.

Pseudonimizzazione: trattamento dei dati personali in modo tale che non possano più essere attribuiti a un interessato specifico senza informazioni aggiuntive conservate separatamente e protette.

Registro interno delle IA: elenco organizzativo dei sistemi e dei casi d'uso autorizzati dall'Ente, contenente le informazioni necessarie alla governance, al monitoraggio e alla rendicontazione.

Registro pubblico delle IA: insieme delle informazioni sui sistemi di IA dell'Ente rese pubbliche per finalità di trasparenza, nei casi e nei limiti previsti dalla Policy e dalla normativa.

Sistema di IA: sistema automatizzato progettato per funzionare con livelli di autonomia variabili, che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dagli input ricevuti come generare output quali previsioni, contenuti, raccomandazioni o decisioni capaci di influenzare ambienti fisici o virtuali.

XAI - Explainable AI: insieme di metodi e tecniche diretti a rendere maggiormente comprensibili il funzionamento o gli output di un sistema di IA, in misura adeguata alle caratteristiche del sistema e ai destinatari.