

PROCEDURA OPERATIVA PER L'USO DI STRUMENTI DI INTELLIGENZA ARTIFICIALE GENERATIVA

ChatGPT – Microsoft Copilot – Google Gemini – Claude e strumenti analoghi

Allegato alla Politica per l'uso responsabile dell'Intelligenza Artificiale

1. Finalità

La presente procedura definisce le regole essenziali che il personale del Comune di Noicattaro deve rispettare nell'utilizzo di strumenti di Intelligenza Artificiale generativa, quali ChatGPT, Microsoft Copilot, Google Gemini, Claude o servizi analoghi.

Gli strumenti di IA possono costituire un utile supporto alle attività lavorative, ma devono essere utilizzati in modo consapevole, sicuro e conforme alla normativa, evitando che informazioni dell'Ente, dati personali o contenuti riservati siano comunicati a servizi non autorizzati.

L'IA costituisce uno **strumento di supporto**: la responsabilità dell'attività svolta, del documento prodotto e delle decisioni assunte resta sempre in capo alla persona competente.

2. Quali strumenti possono essere utilizzati

Per attività istituzionali possono essere utilizzati esclusivamente:

- strumenti espressamente autorizzati dall'Ente;
- versioni, account e configurazioni messi a disposizione dall'Amministrazione;
- eventuali servizi inclusi nell'elenco interno degli strumenti IA autorizzati.

L'autorizzazione riguarda non soltanto il prodotto, ma anche lo **specifico caso d'uso**.

Il fatto che un servizio sia disponibile gratuitamente su Internet o accessibile mediante un account personale non ne autorizza l'utilizzo per finalità lavorative.

È pertanto vietato utilizzare account personali di ChatGPT, Copilot, Gemini o servizi analoghi per caricare o trattare documenti, dati o informazioni dell'Amministrazione non destinati alla pubblica diffusione.

3. Cosa è possibile fare

Salvo differenti disposizioni dell'Ente, gli strumenti IA autorizzati possono essere utilizzati, a titolo esemplificativo, per:

- predisporre una prima bozza di testi, comunicazioni o documenti;
- migliorare la forma linguistica di testi;
- sintetizzare informazioni non riservate;
- tradurre testi;
- organizzare concetti o predisporre schemi;
- generare idee, titoli, indici o strutture di documenti;
- effettuare analisi preliminari di informazioni pubbliche;

- predisporre formule, modelli o esempi;
- supportare attività informatiche o di programmazione, nel rispetto delle verifiche di sicurezza previste;
- elaborare dati anonimi, aggregati o sintetici;
- svolgere attività formative.

L'utilizzo deve comunque essere coerente con le mansioni del dipendente e con le finalità istituzionali dell'Ente.

4. Cosa NON deve essere inserito nei sistemi IA non autorizzati

Nei sistemi di IA pubblici, personali o comunque non espressamente autorizzati dall'Ente **non devono essere inseriti, copiati, allegati o descritti:**

Dati personali

Ad esempio:

- nomi e cognomi associati a pratiche o procedimenti;
- codici fiscali;
- indirizzi;
- numeri di telefono;
- email personali;
- documenti di identità;
- matricole o identificativi individuali;
- dati dei dipendenti;
- dati relativi a cittadini o utenti.

Dati particolari o giudiziari

È vietato inserire, in particolare:

- dati sanitari;
- informazioni sulla disabilità;
- dati biometrici;
- informazioni sull'origine razziale o etnica;
- convinzioni religiose;
- appartenenza sindacale;
- opinioni politiche;
- dati relativi alla vita o all'orientamento sessuale;
- dati relativi a condanne penali, procedimenti penali o reati.

Informazioni riservate dell'Ente

Non devono essere inseriti:

- atti non pubblicati;
- documenti istruttori interni;
- pareri riservati;
- corrispondenza interna;
- PEC non pubbliche;
- documentazione relativa a procedimenti disciplinari;
- informazioni riguardanti gare o procedure in corso, se riservate;
- segnalazioni whistleblowing;
- informazioni concernenti contenziosi;
- informazioni tutelate da segreto d'ufficio;
- documentazione non destinata alla diffusione.

Informazioni di sicurezza

È sempre vietato inserire:

- password;
- PIN;
- chiavi API;
- token;
- credenziali;
- configurazioni di rete;
- vulnerabilità non pubbliche;
- informazioni sulle misure di sicurezza;
- dati relativi a incidenti informatici non pubblici.

5. Dati personali e sistemi IA autorizzati

Il divieto di utilizzare dati personali **non è assoluto**.

Un sistema IA espressamente autorizzato dall'Ente può trattare dati personali quando ciò sia necessario per una finalità istituzionale e siano state preventivamente verificate:

- la base giuridica del trattamento;
- la necessità del dato;
- la proporzionalità;
- la configurazione del servizio;

- la sicurezza;
- il ruolo del fornitore;
- gli eventuali trasferimenti di dati;
- i tempi di conservazione;
- l'eventuale necessità di una DPIA;
- le ulteriori garanzie previste dal GDPR e dalla Policy IA dell'Ente.

Il singolo dipendente **non può decidere autonomamente** di iniziare a utilizzare dati personali con un servizio IA.

In caso di dubbio deve utilizzare dati anonimi o sintetici oppure rivolgersi al proprio responsabile.

6. Prima di inviare un prompt

Prima di utilizzare un sistema IA il dipendente deve chiedersi:

1. Lo strumento è autorizzato dall'Ente?

Se la risposta è NO o non è conosciuta, non devono essere inserite informazioni dell'Amministrazione non pubbliche.

2. Nel prompt sono presenti dati personali o informazioni riservate?

Se Sì, occorre verificare che il relativo utilizzo sia stato espressamente autorizzato.

3. Posso ottenere lo stesso risultato eliminando nomi, identificativi o altri dettagli?

Quando possibile devono essere utilizzati dati anonimi, pseudonimizzati o sintetici.

Esempio da evitare

“Scrivi una risposta al ricorso presentato dal Sig. Mario Rossi, codice fiscale RSSMRA..., residente in..., affetto da...”

Esempio preferibile

“Predisponi uno schema generale di risposta a un'istanza amministrativa avente le seguenti caratteristiche...”

7. Verifica obbligatoria degli output

Gli strumenti di IA possono generare informazioni:

- false;
- inesatte;
- non aggiornate;
- incomplete;
- inventate;
- discriminatorie;
- basate su fonti inesistenti.

Il dipendente deve pertanto **verificare sempre il risultato** prima di utilizzarlo.

Particolare attenzione deve essere prestata a:

Normativa

Non devono essere considerate corrette senza verifica:

- leggi;
- articoli di legge;
- sentenze;
- provvedimenti;
- circolari;
- linee guida;
- termini procedurali.

Le fonti devono essere controllate attraverso banche dati, siti istituzionali o altre fonti attendibili.

Giurisprudenza

Una sentenza o un provvedimento citato dall'IA deve essere verificato.

L'IA può generare numeri, date, massime o riferimenti giurisprudenziali inesistenti.

Dati e statistiche

Numeri, percentuali e statistiche devono essere verificati rispetto alla fonte originaria.

Testi amministrativi

Una bozza generata dall'IA deve essere controllata dal soggetto competente quanto a:

- correttezza giuridica;
- competenza amministrativa;
- elementi istruttori;
- motivazione;
- dati riportati;
- riferimenti normativi.

8. IA e atti amministrativi

L'IA può assistere il personale nella predisposizione di bozze, schemi o analisi.

Non può tuttavia sostituire l'attività istruttoria, valutativa o decisionale del responsabile competente.

La persona che utilizza l'output deve:

- verificarlo;
- modificarlo ove necessario;
- valutarne autonomamente il contenuto;

- assumere la responsabilità del documento finale.

È vietata l'adozione automatica di un output IA quale decisione amministrativa quando manca una reale valutazione umana.

Particolare cautela deve essere utilizzata quando il risultato può incidere sui diritti o sugli interessi di cittadini, dipendenti o imprese.

9. IA e posta elettronica

È possibile utilizzare strumenti autorizzati per supportare la predisposizione di email o comunicazioni.

Prima di inviare contenuti a un sistema IA occorre tuttavia verificare che:

- non siano presenti dati non necessari;
- non siano presenti informazioni riservate;
- eventuali allegati possano essere legittimamente trattati dal servizio;
- il sistema utilizzato sia autorizzato per tale finalità.

Non deve essere copiata integralmente una conversazione email contenente dati personali o informazioni riservate in un servizio IA non autorizzato.

10. File e allegati

Il caricamento di un documento in un sistema IA equivale alla comunicazione del suo contenuto al servizio utilizzato.

Prima di caricare un file il dipendente deve quindi verificare:

- natura del documento;
- presenza di dati personali;
- presenza di dati particolari;
- eventuale riservatezza;
- autorizzazione del sistema a trattare tali informazioni.

La semplice rimozione del nome del file **non anonimizza il contenuto**.

Occorre verificare anche il testo, le tabelle, i metadati e gli eventuali allegati incorporati.

11. Immagini, audio, video e deepfake

Gli strumenti IA possono essere utilizzati per generare o modificare immagini, audio e video esclusivamente per finalità istituzionali autorizzate.

È vietato creare contenuti idonei a:

- rappresentare falsamente dichiarazioni o comportamenti di persone reali;
- ingannare cittadini o utenti;

- compromettere l'immagine o l'affidabilità dell'Ente;
- violare diritti di terzi.

Devono essere rispettati gli eventuali obblighi di informazione o marcatura previsti dalla normativa per i contenuti generati o manipolati artificialmente.

12. Utilizzo dell'IA per codice informatico

Il codice prodotto da strumenti IA deve essere considerato **codice non verificato**.

Prima del suo utilizzo devono essere effettuati i normali controlli di sviluppo sicuro.

In particolare devono essere valutati:

- vulnerabilità;
- dipendenze;
- librerie utilizzate;
- errori;
- credenziali eventualmente incorporate;
- licenze;
- compatibilità con gli standard ICT dell'Ente.

È vietato inserire nei prompt password, token, chiavi API o parti di configurazione che possano compromettere la sicurezza dell'Ente.

13. Casi in cui occorre fermarsi e chiedere autorizzazione

Il dipendente **non deve procedere autonomamente** quando intende utilizzare l'IA per:

- valutare o classificare persone;
- selezionare candidati;
- valutare dipendenti;
- attribuire punteggi;
- determinare priorità tra cittadini;
- formulare graduatorie;
- profilare utenti;
- supportare decisioni che incidono significativamente sulle persone;
- trattare sistematicamente dati personali;
- trattare categorie particolari di dati;
- effettuare riconoscimento biometrico;

- analizzare emozioni o comportamenti;
- integrare un sistema IA con banche dati dell'Ente;
- utilizzare un nuovo sistema o fornitore;
- addestrare o personalizzare modelli con dati dell'Ente.

In questi casi deve essere attivata la procedura di valutazione prevista dalla Policy IA.

14. Come comportarsi in caso di errore o incidente

Il dipendente deve segnalare tempestivamente:

- caricamento accidentale di dati in un sistema non autorizzato;
- diffusione involontaria di dati;
- output gravemente errato utilizzato in attività istituzionali;
- comportamento discriminatorio del sistema;
- accesso non autorizzato;
- malfunzionamento rilevante;
- utilizzo improprio dell'IA;
- sospetta compromissione del servizio.

La segnalazione deve essere effettuata attraverso i normali canali ICT/privacy/incident management dell'Ente e al Referente IA o RTD, ove individuati.

Qualora siano coinvolti dati personali deve essere attivata anche la procedura interna di gestione dei data breach.

15. LE 10 REGOLE DA RICORDARE

- 1. Usa soltanto strumenti IA autorizzati dall'Ente.**
 - 2. Non usare account personali per elaborare documenti o informazioni riservate dell'Amministrazione.**
 - 3. Non inserire dati personali o riservati nei servizi IA pubblici o non autorizzati.**
 - 4. Prima di utilizzare un dato chiediti sempre se puoi eliminarlo, anonimizzarlo o sostituirlo con un esempio.**
 - 5. Non inserire mai password, credenziali, token o informazioni di sicurezza.**
 - 6. Verifica sempre gli output: l'IA può sbagliare o inventare informazioni e fonti.**
 - 7. Verifica direttamente leggi, sentenze, dati e riferimenti normativi.**
 - 8. L'IA può aiutarti a predisporre un atto, ma non può assumere la responsabilità della decisione al tuo posto.**
 - 9. Non utilizzare autonomamente l'IA per valutare, profilare o classificare persone.**
 - 10. In caso di dubbio, non inserire il dato e chiedi indicazioni al tuo responsabile o alle strutture competenti.**
-

REGOLA FINALE

Prima di inviare qualsiasi informazione a un sistema di IA, considera se saresti autorizzato a comunicarla a un soggetto esterno all'Amministrazione.

Se la risposta è negativa o dubbia, l'informazione non deve essere inserita nel sistema salvo che lo strumento sia stato specificamente autorizzato dall'Ente per trattarla e siano state adottate le necessarie garanzie.

SEMAFORO IA

Regole rapide per l'uso di ChatGPT, Copilot, Gemini e strumenti analoghi

**Prima di usare uno strumento di Intelligenza Artificiale chiediti sempre:
"Lo strumento è autorizzato dall'Ente? Posso comunicargli queste informazioni?"**

VERDE – PUOI PROCEDERE

Puoi utilizzare **strumenti IA autorizzati dall'Ente** per attività di supporto quali:

- predisporre bozze di testi, email, comunicazioni e documenti;
- migliorare stile, chiarezza e forma linguistica;
- creare schemi, indici, sintesi e presentazioni;
- tradurre testi;
- generare idee o proposte;
- analizzare informazioni pubbliche;
- elaborare dati anonimi, aggregati o sintetici;
- predisporre esempi, modelli o formulari;
- ottenere supporto preliminare per attività informatiche.

ATTENZIONE

L'output dell'IA **deve sempre essere verificato**.

Controlla in particolare:

norme – sentenze – date – dati – statistiche – citazioni – fonti – nomi – importi.

L'IA può produrre informazioni errate, non aggiornate o completamente inesistenti.

GIALLO – FERMATI E VERIFICA PRIMA

Devi chiedere indicazioni al tuo responsabile o alle strutture competenti prima di utilizzare l'IA quando sono coinvolti:

- dati personali di cittadini o dipendenti;
- documenti amministrativi non pubblicati;

- pratiche o procedimenti in corso;
- dati sanitari o altre categorie particolari di dati;
- dati giudiziari;
- informazioni riservate;
- documenti relativi a gare o contenziosi;
- integrazioni con banche dati dell'Ente;
- valutazione o classificazione di persone;
- selezione o valutazione del personale;
- attribuzione di punteggi o priorità;
- profilazione;
- decisioni che possono incidere sui diritti delle persone;
- addestramento o personalizzazione di sistemi IA con dati dell'Ente.

In questi casi può essere necessaria una preventiva valutazione **AI Act, GDPR, DPIA, FRIA, cybersecurity o procurement**.

PRINCIPIO DI MINIMIZZAZIONE

Prima di inviare un prompt chiediti:

“Posso ottenere lo stesso risultato senza inserire il dato personale?”

Se possibile:

anonimizza – elimina – sostituisci – generalizza.

● ROSSO – NON FARLO

È vietato:

- utilizzare sistemi IA non autorizzati per trattare informazioni riservate dell'Ente;
- utilizzare account personali per caricare documenti o dati istituzionali non pubblici;
- inserire password, PIN, credenziali, token o chiavi API;
- inserire vulnerabilità o configurazioni di sicurezza non pubbliche;
- caricare segnalazioni whistleblowing;
- inserire dati sanitari o giudiziari in piattaforme non autorizzate;
- copiare intere email o fascicoli contenenti dati personali in servizi IA pubblici;
- accettare automaticamente come corretti gli output prodotti dall'IA;
- utilizzare una sentenza, una norma o una fonte suggerita dall'IA senza verificarne l'esistenza;
- lasciare che l'IA assuma autonomamente decisioni amministrative;
- utilizzare l'IA per discriminare, manipolare, profilare illecitamente o adottare pratiche vietate dall'AI Act;

- generare contenuti falsi o ingannevoli attribuiti a persone reali.

LE 5 REGOLE D'ORO

- 1. USA SOLO STRUMENTI AUTORIZZATI.**
- 2. INSERISCI SOLO I DATI STRETTAMENTE NECESSARI.**
- 3. NON INSERIRE INFORMAZIONI RISERVATE IN SISTEMI NON AUTORIZZATI.**
- 4. VERIFICA SEMPRE L'OUTPUT PRIMA DI UTILIZZARLO.**
- 5. LA DECISIONE E LA RESPONSABILITÀ RESTANO UMANE.**

IN CASO DI DUBBIO

NON INSERIRE IL DATO E CHIEDI PRIMA.

Rivolgiti al tuo **Responsabile / Referente IA / RTD / struttura ICT** e, per gli aspetti relativi alla protezione dei dati personali, alle strutture competenti secondo l'organizzazione dell'Ente.

IN CASO DI ERRORE O INCIDENTE

Se hai inserito accidentalmente dati o documenti in un sistema non autorizzato, oppure rilevi un utilizzo improprio dell'IA:

segnala immediatamente l'evento attraverso i canali ICT/privacy/incident management dell'Ente.

L'IA è uno strumento di supporto.

Non sostituisce la competenza, il controllo e la responsabilità della persona.