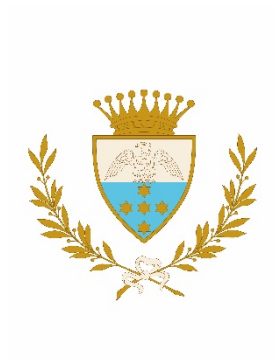


COMUNE DI SALUGGIA

PROVINCIA DI VERCELLI



REGOLAMENTO DELLA RETE COMUNALE, DEL SITO WEB ISTITUZIONALE E DEI SERVIZI DIGITALI DEL COMUNE DI SALUGGIA

INDICE

TITOLO I – DISPOSIZIONI GENERALI

- Art. 1 – Oggetto e finalità
- Art. 2 – Definizioni
- Art. 3 – Riferimenti normativi

TITOLO II – RETE COMUNALE E SITO WEB ISTITUZIONALE

- Art. 4 – Finalità della Rete Comunale
- Art. 5 – Gestione del sito web
- Art. 6 – Accessibilità e usabilità
- Art. 7 – Contenuti e responsabilità
- Art. 8 – Trasparenza e Albo Pretorio

TITOLO III – SPAZI DEDICATI

- Art. 9 – Associazioni del territorio

TITOLO IV – SERVIZI DIGITALI E IDENTITÀ DIGITALE

- Art. 10 – Servizi online ai cittadini
- Art. 11 – SPID, CIE e identità digitale
- Art. 12 – Domicilio digitale

TITOLO V – POSTA ELETTRONICA E PEC

- Art. 13 – Caselle istituzionali
- Art. 14 – Posta Elettronica Certificata (PEC)
- Art. 15 – Sicurezza e limiti d'uso
- Art. 16 – Conservazione e protocollazione

TITOLO VI – ACCOUNT INFORMATICI E SICUREZZA DIGITALE

- Art. 17 – Creazione e gestione degli account
- Art. 18 – Password policy
- Art. 19 – Revoca degli account
- Art. 20 – Logging e monitoraggio
- Art. 21 – Misure minime di sicurezza
- Art. 22 – Gestione degli incidenti informatici

TITOLO VII – SOCIAL MEDIA ISTITUZIONALI

- Art. 23 – Finalità e canali attivi
- Art. 24 – Gestione e responsabilità
- Art. 25 – Regole editoriali
- Art. 26 – Comportamento dei dipendenti sui social media
- Art. 27 – Moderazione e comportamenti non ammessi
- Art. 28 – Trattamento dei dati personali
- Art. 29 – Contenuti multimediali e diritto d'autore

TITOLO VIII – VIDEORIPRESE DEL CONSIGLIO COMUNALE

- Art. 30 – Riprese e trasmissioni
- Art. 31 – Tutela dei dati personali nelle videoriprese
- Art. 32 – Limitazioni e divieti

TITOLO IX – INTELLIGENZA ARTIFICIALE E TECNOLOGIE EMERGENTI

- Art. 33 – Utilizzo di strumenti di intelligenza artificiale

Art. 34 – Pratiche vietate

Art. 35 – Utilizzi ammessi

Art. 36 – Supervisione umana e tracciabilità

Art. 37 – Protezione dei dati personali

Art. 38 – Principi etici, governance e responsabilità

Art. 39 – Governance interna

Art. 40 – Responsabilità del funzionario

Art. 41 – Formazione e aggiornamento

TITOLO X – SANZIONI E RESPONSABILITÀ

Art. 42 – Violazioni e sanzioni disciplinari

Art. 43 – Responsabilità civile e penale

TITOLO XI – DISPOSIZIONI FINALI

Art. 44 – Aggiornamento del regolamento

Art. 45 – Entrata in vigore e abrogazioni

TITOLO I – DISPOSIZIONI GENERALI

Art. 1 – Oggetto e finalità

Il presente Regolamento disciplina l'organizzazione, la gestione e l'utilizzo della Rete Comunale intesa come intranet ed internet, del sito web istituzionale, dei servizi digitali, degli account informatici, della posta elettronica e dei canali di comunicazione istituzionale del Comune di Saluggia.

Il presente Regolamento definisce altresì il quadro generale di principi, ruoli e responsabilità. Le procedure operative di dettaglio, le misure tecniche di sicurezza, le policy applicative e gli allegati tecnici possono essere adottati e aggiornati con atti interni dell'Ente, nel rispetto del presente Regolamento, della normativa vigente e previo coinvolgimento delle figure competenti, ivi compreso il DPO per i profili di protezione dei dati personali.

Le finalità del presente Regolamento sono:

- I. garantire la trasparenza, l'accessibilità e la partecipazione democratica dei cittadini alla vita pubblica;
- II. favorire l'uso consapevole, efficace e sicuro delle tecnologie digitali da parte dell'Ente;
- III. assicurare la corretta gestione dei dati personali nel rispetto del GDPR e della normativa nazionale;
- IV. definire in modo chiaro ruoli, responsabilità e procedure operative per il personale coinvolto;
- V. promuovere la comunicazione istituzionale digitale in modo coerente, professionale e inclusivo;
- VI. adeguare l'Ente alle prescrizioni del Codice dell'Amministrazione Digitale e delle Linee guida AgID.
- VII. Il Comune di Saluggia riconosce il valore strategico della comunicazione digitale quale strumento fondamentale per avvicinare l'istituzione ai cittadini e semplificare l'accesso ai servizi pubblici.

Art. 2 – Definizioni

Ai fini del presente Regolamento si intendono:

Rete Comunale: l'insieme dell'infrastruttura intranet ed internet, dei servizi digitali e delle risorse informative messe a disposizione dal Comune attraverso il sito istituzionale e i canali digitali correlati;

Sito istituzionale: il portale web ufficiale del Comune di Saluggia, accessibile all'indirizzo www.comune.saluggia.vc.it o equivalente, chiaramente ed univocamente riconducibile all'Ente;

Webmaster o fornitore tecnico del sito: il soggetto interno o esterno incaricato delle attività tecniche di gestione, manutenzione, hosting, sicurezza e supporto alla pubblicazione dei contenuti del sito istituzionale. Qualora il soggetto esterno tratti dati personali per conto del Comune, deve essere designato responsabile del trattamento ai sensi dell'art. 28 GDPR;

Referente di servizio o webmaster interno: il dipendente o funzionario individuato dall'Ente come punto di raccordo con il fornitore tecnico e con gli uffici competenti, con funzioni di supervisione operativa e di coordinamento, nei limiti delle autorizzazioni attribuite;

Editor: le figure interne individuate dai Responsabili di servizio e autorizzate alla predisposizione, aggiornamento o pubblicazione dei contenuti sul sito istituzionale, secondo profili di accesso coerenti con le mansioni svolte;

Soggetti autorizzati al trattamento: le persone fisiche che operano sotto l'autorità del Comune o dei responsabili del trattamento e che sono autorizzate a trattare dati personali secondo le istruzioni ricevute e nei limiti delle funzioni assegnate;

DPO o Responsabile della protezione dei dati: il soggetto designato ai sensi degli artt. 37 e seguenti del GDPR, con funzioni di consulenza, informazione, sorveglianza sull'osservanza della normativa e punto di contatto con l'Autorità di controllo, senza attribuzione di compiti gestionali o decisionali sui trattamenti;

Responsabile del trattamento: il soggetto esterno che tratta dati personali per conto del Comune, sulla base di un atto di designazione o di un contratto conforme all'art. 28 GDPR;

Social media istituzionali: i profili/pagine/canali aperti sui social network in nome e per conto del Comune (Facebook, YouTube, Instagram e altri eventualmente attivati);

Account informatico: le credenziali di accesso ai sistemi informatici e/o alle piattaforme software del Comune o utilizzate dall'Ente, assegnate a ciascun utente;

PEC: Posta Elettronica Certificata, con valore legale equiparato alla raccomandata con avviso di ricevimento;

Posta elettronica ordinaria: le caselle di posta elettronica non pec, affidate ai singoli dipendenti o create per la gestione condivisa di servizi;

GDPR: Regolamento (UE) 2016/679 sulla protezione dei dati personali;

SPID: Sistema Pubblico di Identità Digitale;

CIE: Carta di Identità Elettronica;

AgID: Agenzia per l'Italia Digitale;

CAD: Codice dell'Amministrazione Digitale (D.Lgs. 82/2005 e s.m.i.).

Sistema di intelligenza artificiale (IA) integrato: sistema informatico basato su algoritmi di apprendimento automatico, incorporato o interfacciato con le applicazioni gestionali in uso presso l'Ente, in grado di elaborare dati, generare documenti, classificare informazioni o supportare processi decisionali nell'ambito dell'attività amministrativa istituzionale;

Strumento di intelligenza artificiale generativa (IA esterna): servizio o piattaforma di intelligenza artificiale accessibile via web o tramite applicazione, non integrato nell'infrastruttura informatica dell'Ente, che consente la generazione di testi, immagini, sintesi o risposte a partire da richieste in linguaggio naturale (es. assistenti virtuali, motori di ricerca basati su IA, chatbot di terze parti).

Art. 3 – Riferimenti normativi

Il presente Regolamento è adottato nel rispetto e in conformità delle seguenti normative:

- D.Lgs. 7 marzo 2005, n. 82 – Codice dell'Amministrazione Digitale (CAD) e successive modificazioni;
- Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio (GDPR);
- D.Lgs. 30 giugno 2003, n. 196 – Codice in materia di protezione dei dati personali, come modificato dal D.Lgs. 101/2018;
- D.Lgs. 14 marzo 2013, n. 33 – Riordino della disciplina riguardante il diritto di accesso civico e la trasparenza;
- L. 7 agosto 1990, n. 241 – Nuove norme in materia di procedimento amministrativo;
- L. 9 gennaio 2004, n. 4 – Disposizioni per favorire l'accesso dei soggetti disabili agli strumenti informatici (Legge Stanca), come aggiornata dal D.L. 106/2018;
- L. 7 giugno 2000, n. 150 – Disciplina delle attività di informazione e comunicazione delle pubbliche amministrazioni;
- D.P.R. 16 aprile 2013, n. 62 – Codice di comportamento dei dipendenti pubblici;
- Direttiva UE 2016/2102 sull'accessibilità dei siti web e delle applicazioni mobili degli enti pubblici;
- Regolamento (UE) 2024/1689 – Artificial Intelligence Act (Regolamento sull'Intelligenza Artificiale);
- Linee guida AgID su: siti web delle PA, accessibilità, sicurezza ICT, gestione documentale, identità digitale;
- Linee guida AgID per la formazione, gestione e conservazione dei documenti informatici;

- Regolamento (UE) 2024/1689 del 13 giugno 2024 (AI Act), applicabile in via generale dal 2 agosto 2026, con applicazione anticipata dei Capi I e II dal 2 febbraio 2025, di specifiche disposizioni dal 2 agosto 2025 e dell'art. 6, par. 1, con i corrispondenti obblighi, dal 2 agosto 2027;
- Legge 23 settembre 2025, n. 132, recante «Disposizioni e delega al Governo in materia di intelligenza artificiale», in vigore dal 10 ottobre 2025;
- D.Lgs. 82/2005 (Codice dell'Amministrazione Digitale — CAD), D.Lgs. 267/2000 (TUEL), D.Lgs. 165/2001 (TUPI);
- Linee guida, determinazioni e documenti di indirizzo AgID in materia di intelligenza artificiale nella Pubblica Amministrazione, nei limiti in cui risultino definitivamente approvati e applicabili;
- Normativa vigente in materia di PEC, firme elettroniche, SPID e CIE;
- Statuto del Comune di Saluggia e regolamenti comunali vigenti.

TITOLO II – RETE COMUNALE E SITO WEB ISTITUZIONALE

Art. 4 – Finalità della Rete Comunale

- I. La Rete Comunale è il complesso di rete intranet e rete internet che costituisce lo strumento digitale attraverso cui il Comune di Saluggia diffonde informazioni, garantisce l'accesso ai servizi e favorisce la partecipazione dei cittadini alla vita amministrativa.
- II. Il sito istituzionale costituisce il canale ufficiale di comunicazione digitale dell'Ente e rappresenta il punto di riferimento primario per tutti i cittadini, le imprese, le associazioni e gli altri soggetti interessati.
- III. La Rete Comunale persegue le seguenti finalità specifiche:
 - informare i cittadini sulle attività, i servizi e gli atti dell'Amministrazione comunale;
 - garantire il rispetto degli obblighi di pubblicazione e trasparenza previsti dal D.Lgs. 33/2013;
 - favorire l'accesso online ai servizi comunali in conformità al CAD;
 - raccogliere e diffondere informazioni sul territorio, sulle attività culturali, sportive e sociali di interesse pubblico;
 - sostenere la partecipazione democratica e il dialogo tra istituzione e cittadinanza.
 - Mettere al servizio dell'Amministrazione e dei dipendenti comunali una piattaforma sicura e protetta da attacchi al fine di favorire la digitalizzazione delle attività amministrative

Art. 5 – Gestione del sito web

- I. L'ufficio competente del Comune, in attuazione degli indirizzi espressi dalla Giunta Comunale e nel rispetto della normativa sugli affidamenti pubblici, procede all'individuazione di un operatore economico esterno cui affidare, mediante apposito contratto, i servizi di implementazione, gestione tecnica, hosting, manutenzione, sicurezza e supporto redazionale del sito istituzionale. Il contratto disciplina livelli di servizio, misure di sicurezza, continuità operativa, gestione degli accessi, obblighi di riservatezza e, ove necessario, la designazione del fornitore quale responsabile del trattamento ai sensi dell'art. 28 GDPR. È altresì individuato un referente interno all'Ente, con funzioni di supervisione e punto di contatto con il soggetto esterno incaricato.
- II. Il webmaster o fornitore tecnico opera in raccordo con il Segretario Comunale, il Sindaco, i Responsabili di Servizio e l'eventuale Responsabile della Transizione Digitale (RTD) nominato ai sensi

dell'art. 17 del CAD. Il Comune mantiene la responsabilità istituzionale sui contenuti pubblicati e sulle finalità dei trattamenti effettuati tramite il sito.

- III. Ogni ufficio o servizio individua uno o più referenti autorizzati alla predisposizione e alla pubblicazione dei contenuti di competenza. Tali soggetti sono autorizzati al trattamento dei dati personali e ricevono istruzioni adeguate in ordine a correttezza, aggiornamento, accessibilità, riservatezza, minimizzazione e limiti di pubblicazione online.
- IV. Il Comune provvede all'aggiornamento tecnologico e alla manutenzione del sito istituzionale, garantendo continuità del servizio e tempestivo ripristino in caso di disservizi.
- V. Nel caso in cui non sia presente all'interno dell'Ente una figura con competenze adeguate a ricoprire il ruolo di referente tecnico interno, le relative attività di supporto potranno essere richieste alla ditta affidataria nell'ambito dell'affidamento del servizio, ferma restando la distinzione tra responsabilità dell'Ente, compiti del fornitore e funzioni del RTD.

Art. 6 – Accessibilità e usabilità

- I. Il sito web istituzionale rispetta le disposizioni della L. 4/2004, del D.L. 106/2018 e delle Linee guida AgID sull'accessibilità, nonché i requisiti WCAG 2.1 livello AA.
- II. I contenuti devono essere redatti in modo chiaro, semplice e comprensibile, anche da persone con disabilità, conformemente al principio di accessibilità universale.
- III. Il Comune pubblica annualmente, entro il 31 marzo, la Dichiarazione di Accessibilità sul sito istituzionale e sul portale di AgID, con l'indicazione degli eventuali contenuti non accessibili e i relativi rimedi.
- IV. Il sito è ottimizzato per la navigazione da dispositivi mobili (design responsivo) e garantisce tempi di caricamento adeguati.
- V. I documenti pubblicati in formato PDF devono essere, ove possibile, in formato PDF/A accessibile e ricercabile; è vietata la pubblicazione di documenti scansionati non elaborati con OCR.
- VI. Il Comune si impegna a formare il personale addetto alla redazione dei contenuti web sulle buone pratiche di accessibilità.

Art. 7 – Contenuti e responsabilità

- I. I contenuti pubblicati sul sito istituzionale dell'Ente sono finalizzati esclusivamente allo svolgimento delle funzioni istituzionali e all'informazione della cittadinanza. Il sito internet dell'Ente non costituisce in alcun modo strumento di propaganda politica né veicolo per la diffusione di messaggi estranei alle finalità istituzionali; conseguentemente, non è consentita la pubblicazione di contenuti o pagine riconducibili a gruppi politici, movimenti o soggetti portatori di interessi di parte.
- II. I contenuti pubblicati sul sito istituzionale devono essere veritieri, aggiornati, completi, pertinenti e conformi alla normativa vigente.
- III. Quando i contenuti includono dati personali, la pubblicazione deve rispettare i principi di liceità, correttezza, trasparenza, minimizzazione, pertinenza, non eccedenza e limitazione della conservazione. Prima della pubblicazione gli uffici competenti verificano che non siano presenti dati personali non necessari rispetto alla finalità di pubblicazione, con particolare attenzione a dati particolari, dati relativi a minori, dati relativi alla salute, dati giudiziari, indirizzi di residenza, codici fiscali, recapiti personali e informazioni non indispensabili.
- IV. Ogni Responsabile di Servizio è responsabile dell'accuratezza, della completezza e dell'aggiornamento dei contenuti di propria competenza.
- V. I contenuti si distinguono in:
 - i. contenuti statici: informazioni istituzionali stabili nel tempo (organigramma, statuto, regolamenti, recapiti, ecc.);

- ii. contenuti dinamici: notizie, avvisi, bandi, atti, eventi e ogni altra informazione soggetta ad aggiornamento frequente.
- VI. I contenuti statici devono essere verificati e aggiornati dalle varie aree, almeno una volta ogni anno. I contenuti dinamici devono essere aggiornati tempestivamente, comunque entro cinque giorni lavorativi dall'evento che li genera.
- VII. I contenuti pubblicati che non rispettino i requisiti di cui al presente articolo possono essere rimossi o rettificati dal webmaster, previo avviso al Responsabile di Servizio competente.
- VIII. È vietata la pubblicazione di contenuti pubblicitari o promozionali di soggetti privati, salvo i casi espressamente previsti da norme di legge o da specifici accordi istituzionali.
- IX. I contenuti relativi a procedimenti amministrativi devono indicare il responsabile del procedimento, i termini e le modalità di conclusione, in conformità alla L. 241/1990.
- X. La responsabilità dell'ufficio competente comprende anche la verifica preventiva degli allegati e dei documenti pubblicati, nonché l'eventuale oscuramento o estrazione delle sole parti pubblicabili quando la pubblicazione integrale risulti non necessaria o non proporzionata.

Art. 8 – Trasparenza e Albo Pretorio Online

- I. La sezione «Amministrazione Trasparente» è gestita in conformità al D.Lgs. 33/2013, al Piano Nazionale Anticorruzione (PNA) e al Piano Triennale di Prevenzione della Corruzione e Trasparenza (PTPCT) del Comune.
- II. Gli uffici garantiscono la tempestiva pubblicazione di tutti gli atti e le informazioni obbligatori per legge, nel rispetto dei termini di pubblicazione previsti.
- III. L'Albo Pretorio Online è gestito tramite applicativo informatico dedicato, con procedure che garantiscono l'autenticità e l'integrità degli atti pubblicati, la certezza della data di pubblicazione e il rispetto dei termini di legge.
- IV. Ogni Area, per la parte di propria competenza, cura la gestione dell'Albo Pretorio Online, assicurando che gli atti siano resi consultabili secondo le previsioni di legge e nei limiti necessari alla finalità di pubblicazione, previa verifica dell'eventuale presenza di dati personali non pertinenti o eccedenti e con oscuramento dei dati non necessari. Gli allegati agli atti sono pubblicati integralmente solo quando ciò sia previsto o necessario rispetto alla finalità di pubblicazione. In caso contrario, l'ufficio competente valuta la pubblicazione parziale, l'omissione dell'allegato o l'oscuramento delle informazioni non pubblicabili.
- V. Il Comune designa il Responsabile della Prevenzione della Corruzione e della Trasparenza (RPCT), che vigila sull'osservanza degli obblighi di pubblicazione.
- VI. Qualsiasi soggetto può esercitare il diritto di accesso civico semplice o generalizzato secondo le modalità previste dal D.Lgs. 33/2013 e dal regolamento comunale sull'accesso.
- VII. Decorsi i termini di pubblicazione previsti dalla normativa di riferimento, gli atti e i dati personali pubblicati all'Albo Pretorio non devono rimanere indicizzati o liberamente reperibili oltre quanto necessario, fatte salve le diverse regole applicabili alla sezione Amministrazione Trasparente, alla conservazione documentale e agli archivi dell'Ente.

TITOLO III – SPAZI DEDICATI

Art. 9 – Associazioni del territorio

- I. Il Sito Internet dell'Ente può prevedere un apposito calendario per le associazioni ufficialmente costituite e riconosciute, differente rispetto al calendario istituzionale.
- II. Le associazioni regolarmente iscritte al registro comunale delle associazioni, o che intrattengono rapporti formalizzati con il Comune (convenzioni, patrocinii, ecc.), possono richiedere la pubblicazione di un evento da loro organizzato sull'apposito calendario.

- III. La richiesta deve essere inoltrata per iscritto tramite mail dedicata a tale scopo e collegata all'apposito calendario e verrà successivamente validata dal Webmaster interno.
- IV. Sono vietati contenuti a carattere commerciale, politico-partitico, contrari ai principi dell'ordinamento o lesivi di diritti di terzi.
- V. Il Comune può rifiutare la pubblicazione di contenuti non conformi ai criteri del presente articolo o non pertinenti con le finalità istituzionali, senza che ciò costituisca discriminazione.
- VI. Secondo quanto stabilito dall'Art. 7 comma I del presente regolamento, non vengono messe a disposizione sul sito istituzionale pagine dedicate o spazi aggiuntivi per nessun soggetto al di fuori dell'Ente, compresi i gruppi politici di maggioranza e/o minoranza.
- VII. È consentita la pubblicazione, all'interno di questa sezione del sito, dell'elenco delle associazioni territoriali formalmente costituite e dei relativi recapiti istituzionali o pubblici, evitando la pubblicazione di recapiti personali non necessari o di dati eccedenti rispetto alla finalità informativa.

TITOLO IV – SERVIZI DIGITALI E IDENTITÀ DIGITALE

Art. 10 – Servizi online ai cittadini

- I. Il Comune di Saluggia promuove, in conformità al CAD, la progressiva digitalizzazione dei propri servizi, con l'obiettivo di rendere disponibili online le istanze, i procedimenti e i pagamenti in via esclusiva o preferenziale rispetto ai canali tradizionali.
- II. I servizi digitali erogati attraverso il sito istituzionale devono rispettare i principi di accessibilità, usabilità e sicurezza, conformemente alle Linee guida AgID e al modello di design dei siti della PA.
- III. Il Comune adotta, ove possibile, soluzioni di interoperabilità con le piattaforme nazionali (ANPR, PagoPA, AppIO, INAD) e regionali, al fine di semplificare il rapporto con il cittadino.
- IV. I pagamenti informatici verso il Comune devono avvenire esclusivamente attraverso la piattaforma PagoPA, in conformità all'art. 5 del CAD.

Art. 11 – SPID, CIE e identità digitale

- I. Il Comune garantisce l'accesso ai propri servizi digitali tramite SPID e CIE, in conformità alle disposizioni del CAD e alle Linee guida AgID.
- II. I servizi che richiedono autenticazione non devono prevedere ulteriori sistemi di login proprietari, salvo motivate eccezioni tecniche da documentare e sottoporre a revisione periodica.
- III. Il Comune favorisce la diffusione e l'utilizzo dell'identità digitale tra i cittadini, anche attraverso campagne informative e attività di sportello.

Art. 12 – Domicilio digitale

- I. Il Comune utilizza il domicilio digitale dei cittadini registrati nell'Indice Nazionale dei Domicili Digitali (INAD) per le comunicazioni aventi valore legale, in conformità all'art. 6-quater del CAD.
- II. Le comunicazioni verso i cittadini privi di domicilio digitale avvengono con le modalità tradizionali, salvo diversa disposizione di legge.
- III. Il Comune promuove la registrazione dei cittadini all'INAD attraverso attività di sensibilizzazione e assistenza allo sportello.

TITOLO V – POSTA ELETTRONICA E PEC

Art. 13 – Caselle istituzionali

Le caselle di posta elettronica costituiscono strumenti di lavoro finalizzati allo svolgimento delle attività istituzionali, amministrative e di comunicazione verso cittadini, imprese e altre pubbliche amministrazioni.

I. Tipologie di caselle di posta

- I. L'Ente adotta le seguenti tipologie di caselle:
 - caselle nominative individuali assegnate al personale dipendente e agli amministratori;
 - caselle funzionali/di servizio associate a uffici o funzioni;
 - indirizzi di tipo alias, liste o gruppi di distribuzione.
- II. Le caselle funzionali o condivise sono ammesse quando rispondono a esigenze organizzative dell'Ente, purché siano gestite con criteri di responsabilità, tracciabilità e sicurezza. L'accesso deve avvenire, ove tecnicamente possibile, tramite credenziali nominative, deleghe profilate o gruppi di distribuzione riconducibili agli utilizzatori autorizzati;
- III. Le caselle generiche o comuni già attive alla data di entrata in vigore del presente Regolamento possono rimanere operative per esigenze organizzative e di gestione dello storico, purché siano ricondotte a un responsabile di servizio e siano progressivamente adeguate a modalità di accesso tracciabili.
- IV. Per tali caselle comuni devono essere adottate misure idonee a garantire la tracciabilità degli accessi e delle operazioni, evitando l'uso indistinto di credenziali condivise e privilegiando, ove possibile, accessi nominativi o strumenti equivalenti.
- V. Il Responsabile del servizio cui afferisce la casella è il referente organizzativo per il corretto utilizzo della stessa, per l'individuazione degli utilizzatori autorizzati e per la verifica periodica della permanenza delle esigenze di accesso.

II. Assegnazione e gestione

- I. Le caselle nominative sono assegnate a tutto il personale con funzioni amministrative e ai componenti della giunta comunale.
- II. Le caselle nominative sono assegnate dal servizio competente (ICT o equivalente) al momento dell'attivazione del rapporto di lavoro o del mandato amministrativo.
- III. Le caselle funzionali e i gruppi di distribuzione sono istituiti su richiesta del responsabile di servizio, previa valutazione organizzativa.
- IV. Ogni casella deve essere riconducibile a uno o più soggetti responsabili, al fine di garantire tracciabilità, sicurezza e continuità operativa.

III. Modalità di utilizzo

- I. Le caselle di posta elettronica istituzionale devono essere utilizzate esclusivamente per finalità connesse all'attività lavorativa e istituzionale.
- II. È vietato l'utilizzo per scopi personali, commerciali o comunque estranei alle funzioni dell'Ente.
- III. Le comunicazioni devono rispettare i principi di correttezza, trasparenza e protezione dei dati personali.

IV. Sicurezza e conservazione

- I. Gli utenti sono responsabili della custodia delle credenziali di accesso e devono attenersi alle politiche di sicurezza informatica dell'Ente.
- II. Le comunicazioni rilevanti ai fini amministrativi devono essere conservate secondo le norme vigenti in materia di gestione documentale e conservazione digitale.
- III. In conformità alla disciplina in materia di protezione dei dati personali e alle indicazioni del Garante sul trattamento dei metadati della posta elettronica nel contesto lavorativo, l'Ente può adottare sistemi di backup, sicurezza e archiviazione tecnica delle caselle, evitando la consultazione generalizzata e indiscriminata dei contenuti e disciplinando tempi, finalità e soggetti autorizzati all'eventuale accesso.

V. Cessazione del mandato degli amministratori

- I. Alla cessazione del mandato amministrativo, le caselle nominative degli amministratori sono mantenute attive per un periodo massimo di 30 giorni, al fine di consentire il passaggio di consegne e la gestione delle comunicazioni pendenti.
- II. Decorso tale termine:
 - a. la casella viene disattivata;
 - b. può essere attivato, per un ulteriore periodo massimo di 90 giorni, un sistema di risposta automatica con indicazione dei nuovi riferimenti istituzionali;
- III. Le caselle funzionali riferite a cariche o funzioni istituzionali, quali **sindaco@comune.saluggia.vc.it** e **segretario@comune.saluggia.vc.it**, rimangono attive per garantire la continuità dell'azione amministrativa. Al cambio del titolare della carica o della funzione, l'Amministratore di sistema procede tempestivamente alla modifica delle credenziali e alla verifica degli accessi autorizzati, secondo una procedura documentata.

VI. Cessazione del rapporto di lavoro (dipendenti)

- I. In caso di cessazione del rapporto di lavoro (dimissioni, pensionamento o altra causa), la casella nominativa è mantenuta attiva per un periodo massimo di 30 giorni, salvo diverse esigenze organizzative motivate.
- II. Durante tale periodo:
 - a. il responsabile di servizio garantisce la presa in carico delle comunicazioni;
 - b. eventuali inoltri automatici o accessi delegati possono essere attivati solo se necessari, proporzionati, temporalmente limitati e documentati, privilegiando messaggi automatici con indicazione dei nuovi riferimenti istituzionali e la presa in carico delle comunicazioni da parte del responsabile di servizio;
- III. Decorso il termine:
 - a. la casella è disattivata;
 - b. può essere mantenuto un messaggio automatico informativo per un massimo di 90 giorni;
- IV. i contenuti di interesse amministrativo sono acquisiti e gestiti dall'Ente secondo le regole di protocollo, fascicolazione e conservazione documentale, evitando l'accesso a comunicazioni non pertinenti o di natura personale eventualmente presenti nella casella.

VII. Continuità operativa

L'Ente assicura la continuità delle comunicazioni istituzionali mediante l'utilizzo di caselle funzionali, alias e gruppi di distribuzione.

- I. In caso di assenza prolungata del titolare, il responsabile di servizio può adottare misure di continuità operativa quali deleghe nominative, messaggi automatici o presa in carico delle comunicazioni istituzionali. L'accesso ai contenuti della casella individuale deve avvenire solo quando necessario, in modo proporzionato e secondo procedura documentata.
- II. È vietata la lettura sistematica o generalizzata della corrispondenza dei dipendenti. Ogni eventuale accesso per esigenze organizzative, di sicurezza, difensive o di continuità amministrativa deve essere fondato su presupposti documentati, proporzionato alla finalità perseguita e conforme alla normativa applicabile in materia di controlli a distanza e protezione dei dati personali.

Art. 14 – Posta Elettronica Certificata (PEC)

- I. La PEC è utilizzata per tutte le comunicazioni ufficiali con valore legale tra il Comune e altri soggetti pubblici o privati, quando previsto dalla normativa o richiesto dalla natura dell'atto.
- II. L'indirizzo PEC istituzionale del Comune è pubblicato sull'Indice delle Pubbliche Amministrazioni (IPA) e sul sito istituzionale.
- III. I messaggi PEC ricevuti con rilevanza giuridico-amministrativa sono protocollati e conservati secondo le Linee guida AgID sulla conservazione dei documenti informatici.
- IV. La ricevuta di avvenuta consegna della PEC costituisce prova dell'invio e della ricezione del messaggio.

Art. 15 – Sicurezza e limiti d'uso

- I. L'utilizzo della posta elettronica istituzionale e della PEC è soggetto ai seguenti divieti assoluti:
 - inviare materiale illecito, offensivo, diffamatorio o non attinente all'attività lavorativa;
 - divulgare a terzi le proprie credenziali di accesso;
 - utilizzare la posta per fini personali, commerciali o politici;
 - effettuare invii massivi non autorizzati (spam);
 - aprire allegati di provenienza sconosciuta o sospetta (phishing);
 - inviare dati personali o informazioni riservate a destinatari non autorizzati;
 - utilizzare indirizzi e-mail personali per comunicazioni ufficiali dell'Ente, salvo situazioni eccezionali e documentate di indisponibilità dei canali istituzionali, da gestire secondo le istruzioni del Responsabile competente e con successivo riversamento nella corretta gestione documentale.
- II. In caso di ricezione di messaggi sospetti o di possibili attacchi di phishing, il dipendente deve darne immediata comunicazione al Responsabile informatico senza aprire allegati o cliccare su link.

Art. 16 – Conservazione e protocollazione

- I. I messaggi di posta elettronica e PEC che costituiscono corrispondenza ufficiale, atti o documenti amministrativi rilevanti devono essere protocollati nel sistema di protocollazione informatica e conservati nel sistema di gestione documentale del Comune.
- II. La conservazione avviene in conformità al Manuale di Gestione Documentale adottato dal Comune e alle Linee guida AgID sulla formazione, gestione e conservazione dei documenti informatici.
- III. I messaggi relativi a procedimenti amministrativi devono essere inseriti nel fascicolo informatico del relativo procedimento.

TITOLO VI – ACCOUNT INFORMATICI E SICUREZZA DIGITALE

Art. 17 – Creazione e gestione degli account

- I. Ogni dipendente, amministratore (componente della giunta comunale) e collaboratore esterno qualificato del Comune che acceda ai sistemi informatici dell'Ente dispone di un account personale nominativo, non trasferibile e non condivisibile.
- II. Gli account sono assegnati secondo il principio del minimo privilegio: ciascun utente accede esclusivamente ai dati e alle funzionalità strettamente necessari all'esercizio delle proprie funzioni.
- III. La creazione degli account è disposta dal Responsabile del Servizio, con richiesta formale al Responsabile informatico, indicando il profilo di autorizzazione richiesto.
- IV. Gli account condivisi tra più utenti sono vietati, salvo motivate eccezioni tecniche documentate e soggette a revisione annuale.
- V. L'account informatico è di proprietà del Comune e deve essere utilizzato esclusivamente per finalità lavorative istituzionali.
- VI. Tali principi si applicano sia per l'accesso ai dispositivi dell'Ente (account computer) che agli applicativi necessari allo svolgimento della propria prestazione lavorativa.

Art. 18 – Password policy

- I. L'Ente adotta politiche di autenticazione coerenti con le misure di sicurezza applicabili e con il principio del rischio, prevedendo password robuste, divieto di riutilizzo e condivisione delle credenziali, cambio delle credenziali nei casi di compromissione o avvicendamento, autenticazione a più fattori ove disponibile o necessaria e riesame periodico degli accessi privilegiati.

Art. 19 – Revoca degli account

- I. Alla cessazione del rapporto di lavoro, del mandato amministrativo o della collaborazione, l'account informatico individuale del dipendente, amministratore o collaboratore è disattivato tempestivamente e comunque entro il primo giorno lavorativo utile dalla comunicazione della cessazione, salvo esigenze tecniche documentate e limitate al tempo strettamente necessario.
- II. In caso di cambio di mansioni o di ufficio, i privilegi di accesso sono rivisti e aggiornati entro 5 giorni lavorativi.
- III. Il Responsabile di Servizio è tenuto a comunicare tempestivamente al Responsabile informatico qualsiasi variazione nel rapporto di lavoro che comporti la modifica o la revoca degli account.
- IV. Gli account disattivati sono conservati o cancellati secondo le esigenze tecniche, documentali e di sicurezza dell'Ente. I dati e i documenti di rilevanza amministrativa devono essere previamente ricondotti ai sistemi documentali o agli archivi dell'Ente, nel rispetto dei tempi di conservazione applicabili.
- V. Gli account nominativi dei singoli assessori sono disattivati secondo quanto previsto dal comma I del presente articolo. Gli account funzionali riferiti a cariche istituzionali, ove presenti, non sono utilizzati come account personali e sono gestiti con rotazione delle credenziali e aggiornamento degli accessi al cambio della carica.

Art. 20 – Logging e monitoraggio

- I. Il sistema informatico del Comune registra gli accessi e le operazioni rilevanti effettuate dagli utenti (log di sistema), nel rispetto delle disposizioni del GDPR e delle Linee guida del Garante per la protezione dei dati personali.

- II. I tempi di conservazione dei log sono definiti in modo differenziato in base alla tipologia di log, alla finalità del trattamento, al livello di rischio e alle norme o linee guida applicabili. L'accesso ai log è limitato ai soggetti tecnicamente autorizzati per finalità di sicurezza, continuità operativa, audit o accertamento di anomalie. Il DPO può essere coinvolto per valutazioni, audit o incidenti rilevanti ai fini privacy, ma non è soggetto ordinariamente incaricato della consultazione operativa dei log.
- III. I log non possono essere utilizzati per un controllo sistematico, massivo o preventivo dell'attività dei lavoratori. Eventuali verifiche riferibili all'attività lavorativa devono avvenire nel rispetto dei principi di liceità, trasparenza, proporzionalità, minimizzazione, previa adeguata informazione agli interessati e nel rispetto dell'art. 4 della L. 300/1970, ove applicabile.
- IV. I metadati relativi all'uso della posta elettronica e degli strumenti digitali sono trattati solo per finalità determinate, esplicite e legittime, con tempi di conservazione proporzionati e con misure idonee a evitare forme di monitoraggio non necessario dell'attività dei dipendenti.

Art. 21 – Misure minime di sicurezza

- I. Il Comune adotta le misure minime di sicurezza ICT previste dalla normativa vigente e dalle Linee guida AgID, e si conforma progressivamente alle raccomandazioni del Framework Nazionale per la Cybersecurity e la Data Protection.

Art. 22 – Gestione degli incidenti informatici

- I. In caso di incidente informatico, quale attacco ransomware, accesso non autorizzato, perdita di disponibilità dei sistemi, compromissione di credenziali o altra anomalia rilevante, il dipendente che ne viene a conoscenza deve darne immediata comunicazione al Responsabile informatico o al referente indicato nella procedura interna. Il Responsabile informatico informa tempestivamente il Segretario Comunale, il Responsabile del servizio interessato e il DPO quando l'evento possa comportare una violazione di dati personali.
- II. Quando l'incidente comporta una violazione di dati personali, il Comune, quale titolare del trattamento, attiva la procedura di gestione dei data breach, documenta l'evento, valuta il rischio per i diritti e le libertà degli interessati, acquisisce il supporto del DPO e decide sull'eventuale notifica al Garante e sull'eventuale comunicazione agli interessati nei termini previsti dal GDPR.

Gli incidenti e le violazioni sono registrati in apposito registro interno, con indicazione delle cause, degli effetti, delle misure adottate e delle azioni correttive, anche quando non sia dovuta la notifica all'Autorità di controllo.

TITOLO VII – SOCIAL MEDIA ISTITUZIONALI

Art. 23 – Finalità e canali attivi

- I. Il Comune di Saluggia utilizza i social media come strumento complementare alla comunicazione istituzionale, al fine di informare, coinvolgere e dialogare con la cittadinanza in modo tempestivo, diretto e meno formale.
- II. I social media istituzionali non sostituiscono i canali ufficiali di comunicazione e pubblicazione (sito istituzionale, Albo Pretorio, PEC) ma li integrano.
- III. I canali social media attivi al momento dell'adozione del presente Regolamento sono:
 - Pagina Facebook ufficiale del Comune di Saluggia;
 - Pagina Instagram ufficiale del Comune di Saluggia;

- Canale YouTube ufficiale del Comune di Saluggia.
- IV. L'apertura di nuovi canali, la chiusura di quelli esistenti o l'attivazione di profili tematici deve essere autorizzata dalla Giunta Comunale, su proposta del Sindaco o dell'Ufficio Comunicazione. I nuovi canali attivati sono inseriti nell'elenco allegato al presente Regolamento, che viene aggiornato senza necessità di delibera.
- V. Tutti i profili istituzionali devono contenere il logo ufficiale del Comune e il collegamento al sito istituzionale.

Art. 24 – Gestione e responsabilità

- I. La gestione dei canali social media istituzionali può essere affidata, secondo le indicazioni della Giunta Comunale e nel rispetto degli atti organizzativi dell'Ente, alle seguenti figure:
 - a. Personale interno addetto alla comunicazione;
 - b. Fornitore esterno incaricato della comunicazione istituzionale, da contrattualizzare formalmente e, ove tratti dati personali per conto del Comune, da designare responsabile del trattamento ai sensi dell'art. 28 GDPR;
 - c. Sindaco o assessori da Egli appositamente delegati, nei limiti delle funzioni istituzionali e delle autorizzazioni conferite;
- II. I contenuti devono essere verificati prima della pubblicazione, in modo da garantirne la correttezza, la pertinenza e la conformità al presente Regolamento.
- III. Ciascun gestore dei canali social opera secondo le istruzioni ricevute, risponde del proprio operato secondo l'assetto organizzativo dell'Ente e deve garantire correttezza, sicurezza, riservatezza e coerenza istituzionale delle pubblicazioni.
- IV. Non è consentito l'accesso ai profili istituzionali da dispositivi personali non autorizzati. Le credenziali di accesso sono custodite in modo sicuro, non sono divulgate e devono essere protette con misure adeguate, inclusa l'autenticazione a più fattori ove disponibile.
- V. I profili istituzionali vengono monitorati nei giorni e negli orari lavorativi.

Art. 25 – Regole editoriali

- I. Sono ammessi i seguenti contenuti:
 - informazioni istituzionali, comunicati e avvisi di pubblica utilità;
 - eventi, iniziative culturali, sportive e sociali di interesse collettivo;
 - foto e video di eventi pubblici organizzati o patrocinati dal Comune;
 - link ad atti, documenti e pagine del sito istituzionale;
 - informazioni di emergenza e protezione civile;
 - contenuti relativi a servizi comunali e procedimenti amministrativi.
- II. Sono tassativamente vietati i seguenti contenuti:
 - contenuti di propaganda politica, elettorale o di partito;
 - contenuti pubblicitari o promozionali di soggetti privati non patrocinati dall'Ente;
 - contenuti che violino la privacy di persone fisiche o che divulgino dati personali non autorizzati;
 - contenuti offensivi, discriminatori, diffamatori o lesivi della dignità della persona;
 - contenuti che violino il diritto d'autore o altri diritti di proprietà intellettuale.
- III. Il linguaggio utilizzato deve essere semplice, inclusivo, rispettoso e appropriato al contesto istituzionale.

Art. 26 – Comportamento dei dipendenti sui social media

- I. I dipendenti del Comune che utilizzano i social media a titolo personale devono essere consapevoli che possono essere identificati come dipendenti dell'Ente e sono pertanto tenuti a mantenere un comportamento corretto e rispettoso delle norme del codice di comportamento.
- II. I dipendenti non possono utilizzare profili personali per rilasciare dichiarazioni ufficiali a nome del Comune o per divulgare informazioni riservate o notizie non ancora rese pubbliche dall'Ente.
- III. I dipendenti non possono pubblicare contenuti che danneggino l'immagine del Comune, dei colleghi, degli amministratori o dei cittadini, né contenuti che possano essere interpretati come violazione del segreto d'ufficio.
- IV. Le violazioni del presente articolo sono valutate ai fini disciplinari in conformità al D.P.R. 62/2013 e al codice di comportamento del Comune.

Art. 27 – Moderazione e comportamenti non ammessi

- I. I gestori dei profili istituzionali effettuano la moderazione a posteriori dei commenti e dei contenuti pubblicati dagli utenti.
- II. Non sono ammessi commenti o contenuti degli utenti che:
 - contengano insulti, minacce, linguaggio offensivo o scurrile;
 - abbiano carattere discriminatorio rispetto a genere, orientamento sessuale, età, origine etnica, religione o convinzioni personali;
 - contengano diffamazioni, falsità o informazioni fuorvianti;
 - includano spam, messaggi commerciali non richiesti o link a contenuti illeciti;
 - violino la privacy di terzi divulgandone dati personali non autorizzati;
 - costituiscano comportamenti reiteratamente polemici senza scopo costruttivo (trolling).
- III. I contenuti non conformi possono essere rimossi senza preavviso. In caso di violazioni gravi o reiterate, l'utente può essere bloccato dai profili istituzionali e, se necessario, segnalato all'autorità giudiziaria competente.
- IV. I gestori non sono tenuti a rispondere ai commenti o ai messaggi privati in tempi predeterminati, ma si impegnano a garantire risposte tempestive nei giorni lavorativi.

Art. 28 – Trattamento dei dati personali

- I. Il trattamento dei dati personali degli utenti che interagiscono con i profili social istituzionali avviene in conformità al GDPR e alla privacy policy delle singole piattaforme.
- II. Il Comune non effettua profilazione degli utenti attraverso i canali social istituzionali e non utilizza i dati raccolti per finalità diverse da quelle istituzionali.
- III. Eventuali dati personali ricevuti attraverso messaggi privati sui social sono trattati esclusivamente per rispondere alla richiesta dell'utente o per indirizzarla al canale istituzionale competente. Se il messaggio contiene istanze, segnalazioni, reclami o comunicazioni amministrativamente rilevanti, il gestore invita l'utente a utilizzare i canali ufficiali o trasferisce la comunicazione all'ufficio competente secondo le regole di protocollo e gestione documentale, nei limiti consentiti dalla natura della comunicazione.
- IV. Il Responsabile del servizio competente assicura il corretto trattamento dei dati personali nell'ambito dell'attività sui social media. Il DPO è coinvolto per pareri, verifiche e supporto nei casi rilevanti, senza assumere compiti operativi di gestione dei canali.

Art. 29 – Contenuti multimediali e diritto d'autore

- I. Le immagini, i video e gli altri materiali multimediali pubblicati sui canali social istituzionali devono rispettare la normativa sul diritto d'autore (L. 633/1941 e D.Lgs. 68/2003).

- II. Le immagini che ritraggono persone fisiche devono essere acquisite e pubblicate nel rispetto della normativa in materia di protezione dei dati personali, diritto all'immagine e comunicazione istituzionale. La pubblicazione deve essere collegata a finalità istituzionali, limitata a quanto necessario e preceduta da adeguata informativa, evitando primi piani o dettagli identificativi non indispensabili.
- III. Per le immagini di minori è richiesta una valutazione rafforzata di necessità e proporzionalità e, quando la pubblicazione non sia fondata su specifica previsione normativa o su altra idonea base giuridica, il consenso esplicito di chi esercita la responsabilità genitoriale, con modalità chiare e documentabili.
Il consenso alla pubblicazione di immagini o video deve essere distinto rispetto alla mera partecipazione all'evento e deve indicare i canali di diffusione previsti, quali sito istituzionale, social media o materiale informativo dell'Ente.
- IV. Non è consentito l'utilizzo di immagini o video di proprietà di terzi senza la necessaria autorizzazione o licenza d'uso.

TITOLO VIII – VIDEORIPRESE DEL CONSIGLIO COMUNALE

Art. 30 – Riprese e trasmissioni

- I. Le sedute pubbliche del Consiglio Comunale possono essere videoregistrate e trasmesse in diretta o in differita attraverso i canali istituzionali individuati dall'Ente, secondo quanto stabilito dal Regolamento per il funzionamento del Consiglio Comunale e dagli atti organizzativi adottati dall'Amministrazione.
- II. Al fine di garantire qualità tecnica, continuità del servizio, sicurezza e adeguata gestione delle registrazioni, il servizio di registrazione audio, ripresa video e trasmissione può essere affidato a un operatore esterno con comprovata professionalità nel settore, da contrattualizzare formalmente e, ove necessario, da designare responsabile del trattamento.
- III. L'affidamento esterno è motivato dall'esigenza di assicurare neutralità operativa e continuità organizzativa del servizio, dal rispetto di quanto previsto dall'art. 6 del DPR 62/2013, e evitando di attribuire al personale interno compiti tecnici non coerenti con le risorse disponibili o con l'assetto organizzativo dell'Ente.
- IV. Le registrazioni delle sedute pubbliche sono pubblicate e conservate per un periodo predeterminato dall'Ente, coerente con le finalità di trasparenza, documentazione dell'attività consiliare, archiviazione e disponibilità tecnica dei canali utilizzati.
- V. La cancellazione o rimozione dalle piattaforme di streaming non può dipendere esclusivamente da esigenze generiche di spazio disponibile, ma deve avvenire secondo criteri preventivamente definiti, documentati e coerenti con le regole di conservazione documentale e con le finalità di pubblicazione.

Art. 31 – Tutela dei dati personali nelle videoriprese

- I. Le riprese sono sospese o escluse ogniqualvolta il Presidente del Consiglio disponga la riunione in seduta segreta o quando la trattazione comporti la diffusione non necessaria di categorie particolari di dati personali ai sensi dell'art. 9 GDPR, di dati relativi a condanne penali e reati ai sensi dell'art. 10 GDPR, di dati di minori o di altre informazioni riservate non compatibili con la diffusione pubblica.
- II. I soggetti estranei all'Ente eventualmente chiamati a intervenire sono informati prima dell'avvio delle riprese. Quando l'intervento non richiede la ripresa identificabile della persona, devono essere

privilegiare modalità di inquadratura non ravvicinata o comunque proporzionate alla finalità di documentazione della seduta.

- III. Le riprese del pubblico in tribuna sono limitate alle inquadrature generali; è vietata la ripresa ravvicinata e identificabile dei singoli astanti senza consenso.
- IV. Il trattamento dei dati personali derivante dalle videoriprese è disciplinato nell'apposita informativa resa disponibile sul sito istituzionale.

Art. 32 – Limitazioni e divieti

- I. È vietata la diffusione di versioni manipolate, tagliate o alterate delle videoriprese consiliari, che possano travisare il senso degli interventi o delle deliberazioni.
- II. Il download e la redistribuzione delle registrazioni a fini di propaganda politica, elettorale o commerciale sono vietati.
- III. Le registrazioni pubblicate **non** possono essere alterate, manipolate o riutilizzate in modo tale da ledere diritti di terzi, travisare il contenuto degli interventi, perseguire finalità commerciali non autorizzate o violare la normativa applicabile in materia di protezione dei dati personali, diritto d'autore, comunicazione istituzionale e correttezza dell'informazione.

TITOLO IX – INTELLIGENZA ARTIFICIALE E TECNOLOGIE EMERGENTI

Art. 33 – Utilizzo di sistemi di intelligenza artificiale

- I. Ai fini del presente articolo, per sistema di intelligenza artificiale si intende qualsiasi sistema automatizzato progettato per operare con livelli variabili di autonomia, che produce output quali previsioni, raccomandazioni, decisioni o contenuti, tali da influenzare ambienti reali o virtuali, così come definito dal Regolamento (UE) 2024/1689 (AI Act).
- II. L'utilizzo di sistemi di intelligenza artificiale (di seguito «IA») da parte del personale e degli organi del Comune è disciplinato dal presente regolamento e dal quadro normativo richiamato in premessa.
- III. Il presente Regolamento consente l'adozione, con atti interni aggiornabili senza necessità di modifica consiliare, di procedure operative, allegati tecnici, istruzioni al personale e misure organizzative necessarie ad adeguare l'Ente all'evoluzione normativa e tecnologica in materia di intelligenza artificiale.

Art. 34 - Pratiche vietate

- I. È fatto divieto assoluto di utilizzare sistemi di IA che determinano un rischio inaccettabile ai sensi del Capo II dell'AI Act, operativo dal 2 febbraio 2025. In particolare, sono vietati:
 - sistemi di IA che utilizzano tecniche subliminali, ingannevoli o di manipolazione comportamentale nei confronti dei cittadini;
 - sistemi di social scoring che valutino o classifichino persone fisiche in base al comportamento sociale o a caratteristiche personali;
 - sistemi di identificazione biometrica remota in tempo reale negli spazi pubblici (es. riconoscimento facciale), salvo le eccezioni tassativamente previste dall'AI Act;
 - sistemi che sfruttino le vulnerabilità legate all'età, alla disabilità o alla condizione socio-economica dei soggetti.

Art. 35 - Utilizzi ammessi

- I. Il Comune di Saluggia può adottare sistemi di IA a supporto delle attività istruttorie, redazionali e gestionali, con particolare riferimento a:
 - redazione e revisione di atti, comunicazioni e documenti amministrativi, in funzione di supporto al funzionario responsabile;
 - classificazione, smistamento e gestione automatizzata dei flussi documentali;
 - ricerca e sintesi di informazioni normative e giurisprudenziali;
 - analisi di dati aggregati a supporto della pianificazione e della valutazione delle politiche pubbliche;
 - assistenza ai cittadini tramite sistemi di interazione automatizzata (chatbot), nel rispetto degli obblighi di trasparenza di cui all'art. 50 dell'AI Act.

Art.36 - Supervisione umana e tracciabilità

- I. Ogni output prodotto da un sistema di IA — sia esso una bozza di atto, una raccomandazione o qualsiasi altro elaborato — deve essere sottoposto a verifica, valutazione critica e convalida da parte del funzionario o del dirigente responsabile prima di qualsiasi utilizzo ufficiale.
- II. Il dipendente non può limitarsi a recepire acriticamente i risultati forniti dal sistema.
- III. In conformità all'art. 14 della Legge n. 132/2025, qualora un sistema di IA abbia contribuito in modo significativo alla redazione di un atto amministrativo, tale circostanza deve essere indicata nella documentazione di ufficio. La dichiarazione non è richiesta per utilizzi meramente accessori (es. correzione ortografica).

Art. 37 - Protezione dei dati personali

- I. È consentito utilizzare sistemi di IA esterni all'infrastruttura dell'Ente, in particolare strumenti di IA generativa accessibili via web o in cloud non qualificato, esclusivamente per attività di consultazione, supporto redazionale o reperimento di informazioni che non comportino l'inserimento di dati personali, informazioni riservate, segreti d'ufficio o contenuti non destinati alla diffusione pubblica.
- II. È vietato inserire in sistemi di IA esterni all'infrastruttura dell'Ente — in particolare in sistemi di IA generativa accessibili via web o in cloud non qualificato — le seguenti tipologie di informazioni:
 - dati personali comuni o particolari ai sensi degli artt. 4 e 9 del GDPR;
 - dati coperti da segreto d'ufficio, istruttorio o professionale;
 - dati relativi a procedimenti penali, disciplinari o sanzionatori;
 - qualsiasi informazione riservata riguardante cittadini, dipendenti o terzi.
- III. Prima dell'acquisizione o dell'attivazione di qualsiasi sistema di IA, il Responsabile dell'Area competente, in raccordo con il RTD e con il supporto del DPO per i profili di protezione dei dati personali, effettua una valutazione preliminare della finalità, della base giuridica, dei dati trattati, dei rischi, della classificazione del sistema ai sensi dell'AI Act e delle misure tecniche e organizzative necessarie;
- IV. Quando l'adozione di sistemi di IA comporta il trattamento di dati personali, il Comune, quale titolare del trattamento, valuta se ricorrano i presupposti per una Valutazione d'Impatto sulla Protezione dei Dati (DPIA) ai sensi dell'art. 35 GDPR, acquisendo il parere del DPO. I contratti con i fornitori di sistemi di IA devono contenere clausole adeguate in materia di protezione dei dati, sicurezza, localizzazione e trasferimento dei dati, subfornitori, trasparenza, audit, cancellazione o restituzione dei dati e conformità all'AI Act, con chiara indicazione dei ruoli privacy.

Art. 38 – Principi etici, governance e responsabilità

- I. L'adozione e l'utilizzo di sistemi di IA nell'attività amministrativa comunale è ispirata ai seguenti principi fondamentali, in conformità all'art. 14 della Legge n. 132/2025 e all'AI Act:
 - Centralità dell'uomo: l'IA ha un ruolo puramente strumentale; le decisioni restano sempre assunte da una persona fisica, che mantiene la piena responsabilità del procedimento. Nessun atto amministrativo può essere prodotto in via autonoma e definitiva da un sistema di IA;
 - Trasparenza e tracciabilità: i cittadini devono essere informati quando interagiscono con sistemi automatizzati; l'impiego di IA nella formazione degli atti non deve restare invisibile;
 - Non discriminazione: i sistemi automatizzati non devono produrre effetti discriminatori; i dati utilizzati devono essere accurati, aggiornati e rappresentativi;
 - Proporzionalità: l'utilizzo della tecnologia deve essere proporzionato alle finalità perseguite e al livello di rischio del sistema;
 - Responsabilizzazione: la responsabilità delle decisioni amministrative rimane in capo all'essere umano, indipendentemente dagli strumenti utilizzati;
 - Alfabetizzazione: in conformità all'art. 4 dell'AI Act (operativo dal 2 febbraio 2025), il Comune promuove adeguate competenze e consapevolezza in materia di IA per tutto il personale.

Art. 39 - Governance interna

- I. Il Responsabile per la Transizione Digitale (RTD), ai sensi dell'art. 17 del CAD, coordina le attività di adozione e monitoraggio dei sistemi di IA e cura, con il supporto delle Aree competenti, la tenuta di un registro dei sistemi di IA in uso presso l'Ente, contenente almeno: finalità d'uso, unità organizzativa responsabile, fornitore, classificazione di rischio, basi giuridiche e trattamenti di dati personali connessi, misure di supervisione umana e principali misure di sicurezza.
- II. Le decisioni amministrative aventi impatto sui diritti dei cittadini non possono essere adottate in forma esclusivamente automatizzata, ma devono essere sempre validate da un funzionario responsabile.

Art.40 - Responsabilità del funzionario

- I. La supervisione umana e la convalida degli output di IA rientrano nella responsabilità propria del funzionario o del dirigente competente per il procedimento. Il ricorso a un sistema di IA non esonera il dipendente da responsabilità disciplinare, civile o penale per gli atti adottati.
- II. Il personale è tenuto a segnalare tempestivamente al RTD e al Responsabile dell'Area competente qualsiasi anomalia, malfunzionamento o utilizzo improprio di sistemi di IA che possa aver prodotto effetti sugli atti amministrativi o sui dati trattati. Il DPO è coinvolto quando l'anomalia riguarda o può riguardare dati personali, diritti degli interessati o profili di conformità al GDPR.

Art. 41 - Formazione e aggiornamento

- I. In attuazione dell'obbligo di alfabetizzazione previsto dall'art. 4 dell'AI Act e dei principi della Legge n. 132/2025, il Comune promuove:
 - Formazione di base obbligatoria per tutto il personale che utilizza sistemi di IA nell'attività lavorativa, con frequenza almeno annuale;
 - Eventuale formazione specialistica per i dirigenti e i funzionari responsabili di procedimento, con approfondimento dei profili giuridici, etici e tecnici, in relazione all'evoluzione normativa, alle Linee guida AgID e agli indirizzi del Garante per la protezione dei dati personali.

TITOLO X – SANZIONI E RESPONSABILITÀ

Art. 42 – Violazioni e sanzioni disciplinari

- I. Le violazioni del presente Regolamento da parte dei dipendenti comunali, degli amministratori e dei collaboratori costituiscono inosservanza dei doveri d'ufficio e sono soggette alle sanzioni disciplinari previste dalla normativa vigente, dal CCNL di comparto applicabile e dal Codice di comportamento del Comune.
- II. A titolo esemplificativo, costituiscono violazioni del presente Regolamento:
 - l'uso dei sistemi informatici del Comune per finalità estranee al servizio;
 - la divulgazione di credenziali di accesso a terzi;
 - la pubblicazione non autorizzata di contenuti sul sito istituzionale o sui social media;
 - l'omessa segnalazione di incidenti informatici;
 - il mancato aggiornamento dei contenuti di propria competenza;
 - l'utilizzo di strumenti di IA in violazione delle disposizioni del presente Regolamento.
- III. Le sanzioni disciplinari sono irrogate nel rispetto del procedimento disciplinare previsto dalla normativa vigente e, in ogni caso, dopo aver sentito il dipendente interessato.

Art. 43 – Responsabilità civile e penale

- I. Le violazioni del presente Regolamento che integrino illeciti civili o penali sono perseguite nelle sedi competenti, senza che ciò precluda l'esercizio dell'azione disciplinare.
- II. Il Comune può rivalersi nei confronti del dipendente responsabile per i danni eventualmente causati a terzi o all'Ente a seguito di violazione delle disposizioni del presente Regolamento.

TITOLO XI – DISPOSIZIONI FINALI

Art. 44 – Aggiornamento del regolamento

- I. Il presente Regolamento è aggiornato ogni qualvolta intervengano significative modifiche normative o tecnologiche, su proposta del Responsabile della Transizione Digitale (RTD), o del Segretario Comunale.
- II. L'aggiornamento del Regolamento è approvato con deliberazione del Consiglio Comunale. Restano fermi gli aggiornamenti meramente tecnici, procedurali o organizzativi di allegati, policy operative, istruzioni interne e misure di sicurezza, che possono essere adottati con atti interni dell'Ente, purché coerenti con il presente Regolamento e con la normativa vigente.
- III. Il Comune si impegna periodicamente a effettuare una verifica con eventuale revisione organica del presente Regolamento.
- IV. Il Responsabile della Transizione Digitale monitora l'attuazione del Regolamento e propone gli aggiornamenti necessari.

Art. 45 – Entrata in vigore e abrogazioni

- I. Il presente Regolamento entra in vigore il quindicesimo giorno successivo alla sua pubblicazione all'Albo Pretorio Online del Comune di Saluggia.
- II. Dalla data di entrata in vigore del presente Regolamento sono abrogate tutte le disposizioni regolamentari precedentemente adottate dal Comune di Saluggia in materia di rete Comunale, sito

web istituzionale, posta elettronica, account informatici e social media, in quanto incompatibili con le disposizioni del presente Regolamento.

- III. Il presente Regolamento è pubblicato sul sito istituzionale del Comune nella sezione “Regolamenti” e nella sezione «Amministrazione Trasparente – Disposizioni generali – Atti generali».

* * *

Il presente Regolamento è stato approvato con deliberazione del Consiglio Comunale

n. ____ del _____