Comune di Magliano Alfieri

DISCIPLINARE SULL'UTILIZZO DEGLI STRUMENTI INFORMATICI E RELATIVE REGOLE DI COMPORTAMENTO

Premessa

Il Comune di Magliano Alfieri, di seguito «**ente**», riconosce l'importanza assunta dagli strumenti informatici e telematici nell'organizzazione del lavoro, caratterizzando l'azione amministrativa per una maggiore efficacia ed efficienza.

Nonostante l'indubbia semplificazione amministrativa, l'utilizzo improprio delle tecnologie, anche se inconsapevole, pone in pericolo le infrastrutture stesse, le informazioni ed i dati ivi contenuti.

L'utilizzo non corretto degli strumenti informatici può comportare anche la lesione della riservatezza dei dipendenti, degli amministratori o dei terzi. L'azione amministrativa comporta infatti il trattamento di dati personali, alcuni dei quali potrebbero toccare la vita privata o la sfera più personale. L'ente promuove quindi ogni opportuna misura, organizzativa e tecnologica, volta a prevenire il rischio di utilizzi impropri delle strumentazioni e delle banche dati dell'Ente.

Per quanto non specificato nel presente documento è richiesto comunque un atteggiamento ispirato alla correttezza ed alla buona fede.

Capo I – Finalità, ambito di applicazione e principi generali

Art. 1 – Finalità

Il presente disciplinare è finalizzato a definire le modalità di accesso ed utilizzo degli strumenti informatici, della rete informatica e telematica e dei servizi che tramite la stessa rete è possibile ricevere all'interno e all'esterno dell'ente, ai fini di un corretto utilizzo degli strumenti stessi da parte di amministratori, dipendenti o collaboratori, consulenti, stagisti, tirocinanti e soggetti autorizzati dall' ente (di seguito «**utenti**»), i quali dovranno comportarsi seguendo le regole di seguito indicate.

Ulteriore obiettivo è rappresentato dalla volontà di preservare il diritto alla riservatezza degli utenti interni od esterni alla rete informatica e telematica.

Si intende inoltre responsabilizzare gli utilizzatori sulle conseguenze di un uso improprio delle predette strumentazioni.

Per quanto non espressamente previsto dal presente atto, si fa rinvio alle disposizioni generali vigenti in materia (in particolare, il *Codice dell'Amministrazione Digitale, Dlgs 82 del 07/03/2005* e il *Codice di comportamento dei dipendenti pubblici, a norma dell'articolo 54 del decreto legislativo 30 marzo 2001, n. 165, come modificato dal DPR 81 del 13/06/2023*).

Art. 2 – Ambito di applicazione

La rete dell'ente è costituita dall'insieme delle risorse informatiche, cioè dalle risorse hardware e software, e dal patrimonio informativo digitale.

Il patrimonio informativo è l'insieme delle banche dati in formato digitale ed in generale tutti i documenti prodotti tramite l'utilizzo dei suddetti apparati.

Il presente disciplinare si applica a tutti gli utenti autorizzati ad accedere alle risorse tecnologiche del sistema informatico o comunque nella disponibilità dell'ente.

Art. 3 – Principi generali

Il Comune di Magliano Alfieri promuove l'utilizzo della rete informatica e telematica, di internet e della posta elettronica quali strumenti utili a perseguire con efficacia ed efficienza le proprie finalità istituzionali, in accordo con le linee guida ed i principi delineati dalla normativa vigente.

Ogni utente è responsabile, civilmente e penalmente, del corretto uso delle risorse informatiche, dei servizi/programmi a cui ha accesso e dei dati trattati a fini istituzionali. È altresì responsabile del contenuto delle comunicazioni effettuate e ricevute a fini istituzionali anche per quanto attiene la riservatezza dei dati ivi contenuti, la cui diffusione impropria potrebbe configurare violazione del segreto d'ufficio o della normativa per la tutela dei dati personali.

Il lavoratore deve custodire ed utilizzare gli strumenti informatici, internet, la posta elettronica in modo appropriato e diligente ed è responsabile della propria postazione di lavoro.

Sono vietati comportamenti che possono creare un danno, anche d'immagine, all'ente.

CAPO II – CRITERI DI UTILIZZO DEGLI STRUMENTI INFORMATICI E TELEMATICI

Art. 4 – Utilizzo degli strumenti informatici

Gli strumenti informatici (a titolo esemplificativo personal computer, stampante) messi a disposizione degli utenti, costituiscono strumento di lavoro. Pertanto, l'utilizzo di essi da parte degli utenti è consentito per finalità attinenti o comunque connesse con l'attività lavorativa, secondo criteri di correttezza e professionalità, coerentemente al tipo di attività svolta e nel rispetto delle disposizioni normative ed interne e delle esigenze di funzionalità e di sicurezza dei sistemi informativi.

Nella definizione di attività lavorativa sono comprese anche le attività strumentali e collegate alla stessa, quali ad esempio quelle che attengono allo svolgimento del rapporto di lavoro. È escluso qualsivoglia uso per scopi privati e/o personali, ad eccezione dei casi d'urgenza e comunque a condizione che tale uso avvenga in modo non ripetuto o per periodi prolungati.

L'amministrazione, attraverso le proprie figure di vertice e dirigenziali, ha facoltà di svolgere gli accertamenti necessari e adottare ogni misura atta a garantire la sicurezza e la protezione dei sistemi informatici, delle informazioni e dei dati. Le modalità di svolgimento di tali accertamenti sono stabilite mediante linee guida adottate dall'Agenzia per l'Italia Digitale, sentito il Garante per la protezione dei dati personali.
In caso di uso di dispositivi elettronici personali, trova applicazione *l'articolo 12, comma 3-bis del decreto legislativo 7 marzo 2005, n. 82* ove si cita che si favorisce l'uso da parte dei lavoratori di dispositivi elettronici personali o, se di proprietà dei predetti soggetti, personalizzabili, al fine di ottimizzare la prestazione lavorativa, nel rispetto delle condizioni di sicurezza nell'utilizzo.

Art. 5 – Utilizzo del personal computer

L'accesso alla stazione di lavoro è condizionato al corretto inserimento delle credenziali di autenticazione (**nome utente e password**). Per l'uso, la scelta, la modifica e gestione delle credenziali nonché delle password di utilizzo si rinvia anche quanto previsto da schede tecniche e informative dedicate, che dovranno essere rese note agli utenti.

Il personal computer assegnato come postazione di lavoro è configurato con il software necessario al suo utilizzo. Ogni altra installazione, anche di software gratuito e liberamente scaricabile da internet, deve essere previamente autorizzata così come qualsiasi modifica delle configurazioni hardware.

Ogni utente deve tenere comportamenti corretti, tali da preservare il buon funzionamento degli strumenti e tali da ridurre i rischi per la sicurezza del sistema informatico, quali l'utilizzo di supporti per la memorizzazione dei dati non sicuri e CD provenienti dall'esterno, al fine di non diffondere virus.

È vietata l'installazione non autorizzata di hardware che consenta l'accesso non controllato all'esterno della rete comunale (a titolo esemplificativo internet key, chiavi Wireless USB o modem che sfruttino il sistema di comunicazione telefonico per l'accesso a internet o a banche dati esterne).

È vietato copiare o mettere a disposizione di altro materiale protetto dalla legge sul diritto di autore (documenti, files musicali, immagini, filmati e simili) di cui l'ente non abbia acquisito preventivamente i diritti.

Gli applicativi gestionali (Finanziario, Protocollo, Anagrafe, …) sono destinati alla gestione di informazioni il cui utilizzo deve essere compatibile con la disciplina vigente in materia di privacy.

Tutti i dati personali, con particolare attenzione a quelli di natura particolare di cui all'art.9 paragrafo 1 del GDPR – REG UE 2016/679, riprodotti su supporti magnetici o su supporti cartacei devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato, nel rispetto dei principi di cui all'art.5 del GDPR. Non è pertanto consentito, ad esempio, lasciare incustoditi presso le stampanti documenti cartacei contenenti tali dati.

La tutela dei dati archiviati su personal computer che gestiscono localmente documenti e dati è demandata all'utente, il quale dovrà effettuare periodicamente i salvataggi su supporti dedicati e idonei, nonché la conservazione degli stessi in luoghi adatti.

Art. 6 – Credenziali di accesso

L'accesso alle procedure informatiche dell'ente è consentito agli incaricati in possesso di "*credenziali di autenticazione*" che permettano il superamento di una procedura di autenticazione e, se nel caso specifico previsto, di autorizzazione.

Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato (userid o username) associato ad una parola chiave riservata (password). Possono essere utilizzati, allo scopo, strumenti con livelli di sicurezza superiori, quali dispositivi di autenticazione (es. smartcard) biometrici.

Gli incaricati sono responsabili della custodia e dell'utilizzo delle proprie credenziali di autenticazione e devono utilizzarle e gestirle attenendosi alle istruzioni impartite, che possono essere raccolte e specificate in apposite schede tecniche e informative.
Le credenziali di autenticazione individuali per l'accesso alle applicazioni non devono mai essere condivise tra più utenti. Qualora un utente dovesse avere la necessità di trattare dati o usare le procedure, il dirigente o il responsabile del servizio di riferimento potrà richiedere formalmente all'Ente, passando attraverso i soggetti competenti, le relative credenziali di autenticazione, dotate dei privilegi necessari all'accesso ai dati o ai servizi richiesti.

Art. 7 – Utilizzo della rete comunale

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità possono essere svolte regolari attività di controllo e backup da parte degli uffici competenti per l'ente.

L'ente può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà pericolosa per la sicurezza sia sui PC degli incaricati sia sulle unità di rete.

Costituisce *buona regola* la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti da evitare un'archiviazione ridondante.

Art. 8 – Utilizzo della rete internet

L'accesso alla Rete Internet costituisce strumento di lavoro ed è consentito per finalità direttamente attinenti o comunque connesse all'esercizio dell'attività lavorativa. È escluso qualsivoglia uso per scopi privati e/o personali, salvo che tale uso sia motivato da ragioni di urgenza o di necessità. È in ogni caso vietato l'uso reiterato e prolungato per fini personali.

L'ente può adottare misure di filtraggio che permettono di inibire o restringere l'accesso a siti i cui contenuti siano classificati pericolosi o non attinenti agli scopi istituzionali oppure che permettono l'accesso solo a determinati siti la cui consultazione sia stata ritenuta dai singoli Responsabili Informatici utile in relazione agli scopi istituzionali.

Sono vietate azioni idonee ad eludere le misure di filtraggio di cui al precedente comma.

È altresì fermamente **vietato**:

a. **scaricare e/o installare software non espressamente autorizzati dall'ente;**
b. **scaricare e/o usare materiale informatico non direttamente attinenti all'esercizio dell'attività lavorativa;**
c. **scaricare e/o usare materiale informatico il cui contenuto (a mero titolo esemplificativo: software, testo, audio e video) sia coperto da diritto di autore. Nei casi in cui ciò sia necessario per lo svolgimento dell'attività lavorativa, l'utente è tenuto ad attivare preventivamente gli adempimenti previsti dalla legge;**
d. **partecipare a forum di discussione on line, a chat, utilizzare sistemi di chiamata o di video chiamata, ecc. per ragioni non direttamente attinenti o connesse all'attività lavorativa;**
e. **navigare in internet su siti contrari a norme di legge;**
f. **effettuare ogni genere di transazione finanziaria per fini personali;**
g. **installare e utilizzare strumenti per lo scambio di dati attraverso internet con metodologia PEER to PEER (es. torrent, …) indipendentemente dal contenuto dei file scambiati;**
h. **usare i profili social dell'Ente per fini personali, politici o commerciali;**
i. **utilizzare i profili personali attivati sui social media per agire in nome e per conto dell'ente**

Per esigenze di sicurezza delle informazioni dell'ente e per le attività di tutela che gli sono proprie, qualora si ravvisi un traffico anomalo o accessi a siti non connessi ad attività istituzionali o in grado di generare eventi dannosi o situazioni di pericolo o di disfunzioni operative per l'ente, il Comune di Magliano Alfieri può individuarne le cause e l'origine attraverso procedure dedicate di controllo.

Art. 9 – Utilizzo della posta elettronica

L'ente mette a disposizione di ogni utente il servizio di posta elettronica, assegnando a ciascuno di essi caselle di posta istituzionali per fini esclusivamente lavorativi.

Al fine di agevolare lo svolgimento dell'attività lavorativa, l'ente rende disponibili indirizzi di posta elettronica condivisi tra più utenti (caselle di posta istituite per singole unità organizzative) affiancandoli a quelli individuali.

L'indirizzo di posta elettronica messa a disposizione dall'ente, contraddistinto dalla presenza del nome di dominio "*Nome ente.x.it*", costituisce uno strumento di lavoro ed il suo utilizzo è consentito unicamente per finalità attinenti o comunque connesse allo svolgimento dell'attività lavorativa.

È escluso l'uso per scopi privati e/o personali, ad eccezione dei casi d'urgenza e di necessità e comunque non in modo ripetuto.

La sicurezza e la riservatezza della posta elettronica sono garantite dalla necessità di disporre di idonee credenziali di autenticazione per accedere alla stessa. La password dell'account di posta elettronica è scelta e registrata dall'incaricato nel rispetto dei criteri e delle regole che l'ente stesso gli ha indicato attraverso precise istruzioni contenute in schede tecniche e informative dedicate.

Il dipendente è responsabile del contenuto dei messaggi inviati. I dipendenti si uniformano alle modalità di firma dei messaggi di posta elettronica di servizio individuate dall'ente di appartenenza. Ciascun messaggio in uscita deve consentire l'identificazione del dipendente mittente e deve indicare un recapito istituzionale al quale il medesimo è reperibile.

È fatto **divieto** di:

a. **inviare o memorizzare messaggi di natura oltraggiosa, volgare, diffamatoria e/o discriminatoria, ed in ogni caso contrari a norme di legge o idonei a creare danno all' Ente o a terzi; nonché messaggi a catena e/o spam;**
b. **scambiare messaggi impersonando un mittente diverso da quello reale;**
c. **scambiare messaggi di posta contenenti file o link a siti con contenuti illegali, violenti, o pornografici, file o materiale informatico soggetto al diritto d'autore, password e/o codici d'accesso a programmi soggetti a diritto d'autore e/o a siti internet;**
d. **aprire messaggi di posta o allegati di tipo eseguibile, salvo il caso di certezza assoluta dell'identità del mittente e della sicurezza del messaggio;**
e. **inviare, anche da una casella di posta privata, messaggi di natura personale e non attinenti al rapporto di lavoro a indirizzi di posta elettronica contraddistinti dal dominio "nome ente.x.it".**

Qualora si rilevi un utilizzo improprio della posta elettronica da parte di un utente o comunque una violazione delle regole e dei divieti di cui al presente Disciplinare, l'ente informerà l'utente interessato che potrà chiedere di essere ascoltato e di accedere alla relativa documentazione. A seguito delle verifiche effettuate, potranno essere avviati, se del caso, i procedimenti conseguenti.

Art. 10 - Utilizzo dei mezzi di informazione e dei social media

Nell'utilizzo dei propri account di social media, il dipendente utilizza ogni cautela affinché' le proprie opinioni o i propri giudizi su eventi, cose o persone, non siano in alcun modo attribuibili direttamente all'ente di appartenenza.

In ogni caso il dipendente è tenuto ad astenersi da qualsiasi intervento o commento che possa nuocere al prestigio, al decoro o all'immagine dell'ente di appartenenza o della pubblica amministrazione in generale.

Al fine di garantirne i necessari profili di riservatezza le comunicazioni, afferenti direttamente o indirettamente il servizio non si svolgono, di norma, attraverso conversazioni pubbliche mediante l'utilizzo di piattaforme digitali o social media. Sono escluse da tale limitazione le attività o le comunicazioni per le quali l'utilizzo dei social media risponde ad una esigenza di carattere istituzionale.

Le amministrazioni si possono dotare di una "*social media policy*" per ciascuna tipologia di piattaforma digitale, al fine di adeguare alle proprie specificità le disposizioni di cui al presente articolo. In particolare, la "*social media policy*" deve individuare, graduandole in base al livello gerarchico e di responsabilità del dipendente, le condotte che possono danneggiare la reputazione delle amministrazioni.

Fermi restando i casi di divieto previsti dalla legge, i dipendenti non possono divulgare o diffondere per ragioni estranee al loro rapporto di lavoro con l'ente e in difformità alle disposizioni di cui *al decreto legislativo 13 marzo 2013, n. 33, e alla legge 7 agosto 1990, n. 241*, documenti, anche istruttori, e informazioni di cui essi abbiano la disponibilità.

Capo IV – Controlli

Art. 10 – Controlli e responsabilità

Il Comune di Magliano Alfieri si riserva di effettuare controlli sul corretto utilizzo degli strumenti informatici e telematici nel rispetto dei principi di pertinenza e non eccedenza, di correttezza e di gradualità come previsto dalla normativa vigente in tema di protezione dei dati personali.

Per esigenze organizzative, produttive e di sicurezza l'ente può avvalersi di strumenti che consentono un controllo a distanza di tipo generalizzato, indiretto e anonimo, relativo all'intera struttura amministrativa, ad aree, settori o gruppi di utenti. I controlli possono essere attivati a seguito di richiesta del responsabile del servizio o a seguito della rilevazione di anomalie / malfunzionamenti del sistema. Il primo controllo sarà anonimo e nel rispetto del principio di gradualità; qualora – durante un controllo generalizzato – vengano rilevate anomalie nell'utilizzo degli strumenti informatici, l'ente procede preliminarmente all'invio di un avviso generalizzato relativo all'uso improprio riscontrato, con l'invito ad attenersi scrupolosamente al presente Regolamento, e riservandosi la facoltà di svolgere successive azioni mirate alla verifica del corretto utilizzo.

Il mancato rispetto o la violazione delle norme contenute nel presente Regolamento è perseguibile con provvedimenti disciplinari, nonché con le azioni civili e penali consentite.

Art. 11 – Responsabilità degli utenti

L'utente non può in alcun caso modificare la configurazione di rete e non può effettuare manomissioni o interventi sulle apparecchiature o sui programmi non formalmente autorizzati dall'ente, al quale deve comunicare tempestivamente le necessità di interventi su apparecchiature e programmi in ordine alla corretta prestazione dei servizi.
L'accesso alla risorsa informatica è personale e va effettuato tramite nome utente e password di identificazione. L'accesso non può essere condiviso o ceduto. Ove per motivi organizzativi o di prestazione del servizio si rendesse necessaria una condivisione di autenticazioni, tale passaggio dovrà essere autorizzato

o stabilito a monte da parte dell'ente. Gli utenti sono responsabili per la protezione dei dati utilizzati e/o memorizzati nei sistemi in cui hanno accesso; è fatto loro divieto di accedere direttamente o indirettamente a directory, files e servizi ove non espressamente e preventivamente autorizzati dall'ente.

La password è personale e non cedibile o trasmissibile a terzi: è fatto divieto a ciascun utente di divulgare, per fatto imputabile a lui direttamente o indirettamente, password, username e comunque chiavi di accesso riservate. Se smarrite, va fatta immediata segnalazione e richiesta di sostituzione all'ente.

Gli utenti sono obbligati a segnalare immediatamente all'ente ogni sospetto di effrazione, incidente, abuso o violazione della sicurezza.

Gli utenti sono tenuti a mantenersi aggiornati, controllando periodicamente le direttive e le indicazioni fornite dall'ente, tramite comunicazioni di servizio, anche a seguito di indicazioni di specifici soggetti quali il DPO, o Responsabile protezione dei Dati personali.

Capo V – Disposizioni finali

Art. 12 - Violazioni

Il dipendente deve attenersi, nell'utilizzo e nella gestione delle risorse strumentali informatiche comunali, oltre che alle norme del presente disciplinare, ai principi e ai doveri stabiliti nel "*Codice di comportamento dei dipendenti delle pubbliche amministrazioni*".

La violazione da parte dei lavoratori dei principi e delle norme contenute nel presente disciplinare costituisce violazione degli obblighi e dei doveri del dipendente pubblico e, pertanto, in relazione alla gravità dell'infrazione, l'ente, previo espletamento di procedimento disciplinare, potrà procedere all'applicazione delle sanzioni previste dalle disposizioni contrattuali vigenti in materia.