



Comune di Buttiglieria Alta

REGOLAMENTO INTERNO PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI E DI TELECOMUNICAZIONE

1. Premessa	Pag.2
2. Campo di applicazione del Regolamento	Pag. 2
3. Riservatezza dei Dati Personali	Pag. 2
4. Utilizzo del Personal Computer	Pag. 3
5. Gestione e assegnazione delle credenziali di autenticazione	Pag. 4
6. Utilizzo di dispositivi elettronici portatili E BYOD	Pag. 5
7. Uso della posta elettronica	Pag. 5
8. Utilizzo della rete Internet	Pag. 6
9. Protezione antivirus	Pag. 7
10. Partecipazione a social media	Pag. 7
11. Disciplina delle attività di controllo sugli strumenti informatici e telematici	Pag. 8
12. Accesso ai dati trattati dall'utilizzatore	Pag. 9
13. Osservanza delle disposizioni in materia di privacy	Pag. 9
14. Sanzioni	Pag. 9
15. Aggiornamento e revisione	Pag. 10
16. Entrata in vigore e pubblicità del regolamento	Pag. 10

PREMESSA

L'utilizzo in licenza degli strumenti informatici, telematici ed elettronici, hardware e software, server e programmi informatici in uso presso il Comune di Buttiglieria Alta (d'ora innanzi, per brevità, "il Comune") - tutti qualificati, ai sensi dell'art. 4 comma 2 della L. 300/1970 (Statuto dei Lavoratori) come modificato dall'art. 23 D.lgs. 151/2015 "*strumenti per rendere la prestazione lavorativa*"- e dalla stessa forniti e messi a disposizione dei dipendenti e/o collaboratori, comunque contrattualmente qualificati ed ai quali tali strumenti vengono consegnati per rendere prestazioni a favore del Comune (d'ora innanzi definiti per brevità "*utilizzatori*"), nonché l'utilizzo degli strumenti informatici, telematici ed elettronici di proprietà dei collaboratori, comunque contrattualmente qualificati, che vengono autorizzati ad accedere ai dati e servizi informatici/telematici di proprietà del Comune secondo i protocolli e le credenziali di accesso ed autorizzazione dalla stessa definiti, deve sempre ispirarsi ai principi di diligenza e correttezza.

Il Comune, per favorire l'utilizzo corretto, consapevole e sicuro dei predetti strumenti e servizi aziendali da parte degli utilizzatori, ha adottato il presente "Regolamento Interno per l'utilizzo degli strumenti informatici e di telecomunicazione" (di seguito "Regolamento") al fine di assicurare la disponibilità e l'integrità di sistemi informativi e di dati, diretto ad evitare che comportamenti, anche inconsapevoli ed involontari, posti in essere dagli utilizzatori nell'impiego degli strumenti informatici, telematici ed elettronici nell'ambito dell'esecuzione della prestazione lavorativa a favore del Comune, possano determinare, anche a livello puramente potenziale, criticità o minacce alla stabilità del proprio sistema informatico, alla sicurezza nel trattamento dei dati, sia propri che di terzi.

Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni già fornite a tutti gli autorizzati ai fini della tutela dei dati personali ai sensi del Regolamento (UE) 2016/679 (General Data Protection Regulation, d'ora innanzi definito per brevità "GDPR") nonché determinano ed integrano le informazioni già fornite ai dipendenti/interessati in ordine alle finalità e alle modalità dei possibili controlli o alle conseguenze di tipo disciplinare in caso di violazione delle stesse.

CAMPO DI APPLICAZIONE DEL REGOLAMENTO

Il Regolamento si applica:

- a tutti i dipendenti del Comune, senza distinzione di ruolo e/o livello
- a tutti i collaboratori e/o consulenti del Comune, a prescindere dal rapporto contrattuale con lo stesso

che vengano autorizzati a far uso di strumenti informatici di proprietà e forniti dal Comune, ovvero che vengano autorizzati dal Comune ad accedere, conservare e trattare informazioni e applicazioni aziendali mediante dispositivi propri; si parla in tal caso di modalità c.d. BYOD (acronimo di "*Bring Your Own Device*").

Pertanto, il rispetto delle regole di seguito previste deve intendersi a carico di tutti i soggetti di cui al precedente paragrafo (ovvero gli "*utilizzatori*"), ferma restando la necessità che si dia opportuno conto del presente Regolamento nel contratto concluso con questi ultimi, ovvero nella fase immediatamente successiva, ma in ogni caso e comunque prima che l'utilizzatore cominci a rendere la propria prestazione lavorativa a favore del Comune, mediante l'utilizzo dei sistemi informatici e telematici aziendali o propri.

RISERVATEZZA DEI DATI

Tutti i dati memorizzati su computer e sistemi informatici e telematici del Comune, nonché tutti i dati dal Comune memorizzati sui dispositivi di proprietà degli utilizzatori, sono sottoposti a stretta ed esclusiva riservatezza. L'accesso ai dati aziendali da parte degli utilizzatori è concesso e regolato dalle credenziali di autenticazione e dalle autorizzazioni di accesso alla rete, ai servizi e alle infrastrutture informatiche aziendali che ne regolano/limitano il perimetro. L'autorizzazione al trattamento dei dati personali è regolata da specifiche lettere d'autorizzazione fornite dal Comune.

➤ ACCESSO AI DATI AZIENDALI

L'accesso ai dati aziendali può essere revocato e/o limitato a discrezione della direzione del Comune

Tutte le informazioni riservate o limitate devono essere protette dalla divulgazione a terzi. Terze parti possono avere accesso alle informazioni interne solo quando strettamente necessario in relazione alle specifiche esigenze del Comune e previa sottoscrizione di un patto di non divulgazione (c.d. NDA – “*Non Disclosure Agreement*”) approvato dal Comune.

La politica di gestione dei dati e delle informazioni del Comune, anche con riferimento ai trattamenti di dati personali effettuato dal Comune, in accordo con i principi dettati dal GDPR in materia di protezione dei dati personali, si fonda sulla riservatezza e confidenzialità, salvo quando diversamente specificato.

UTILIZZO DEL PERSONAL COMPUTER E DEI DISPOSITIVI DI MEMORIZZAZIONE RIMOVIBILI

Il Personal Computer affidato all'utilizzatore, ovvero l'eventuale dispositivo BYOD utilizzato per rendere la prestazione lavorativa a favore del Comune, è esclusivamente uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza, con conseguente potenziale perdita e/o sottrazione di dati. Il personal computer, così come l'eventuale dispositivo BYOD, deve essere custodito con cura da parte degli assegnatari/proprietari evitando ogni possibile forma di danneggiamento.

Il Personal Computer dato in affidamento all'utilizzatore permette l'accesso alla rete e ai servizi del Comune solo attraverso specifiche credenziali di autenticazione, come meglio *infra* descritto.

➤ INTERVENTI SUL SISTEMA INFORMATICO

Il Comune rende noto che l'Amministratore di Sistema, nella persona del SIG. TRAPANESE ROMEO, è stato autorizzato a compiere interventi sul sistema informatico diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione software e hardware etc.). La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività del Comune, si applica anche in caso di assenza prolungata o impedimento dell'utente.

Qualora lo specifico intervento dovesse comportare anche l'accesso a contenuti delle singole postazioni PC e dispositivi portatili aziendali, l'Amministratore di Sistema ne darà comunicazione agli utilizzatori interessati, preventivamente, ovvero, nel caso di urgenza dell'intervento stesso, contestualmente o nel tempo immediatamente successivo. In caso di necessità di intervento da parte dell'Amministratore di Sistema su dispositivi BYOD, per tutti i motivi tecnici, manutentivi e di sicurezza dei dati aziendali sopra citati, ai fini di tutela della privacy e della protezione dei dati personali, lo stesso dovrà essere limitato alla porzione/area di sistema deputata alla sfera professionale dell'utilizzatore, e dovrà essere effettuato in presenza del proprietario del dispositivo.

In casi di estrema necessità, l'Amministratore di Sistema ha la facoltà di collegarsi e visualizzare in remoto i contenuti delle singole postazioni PC al fine di garantire l'assistenza tecnica, le attività di *patching* e aggiornamento, la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento viene effettuato su chiamata dell'utilizzatore o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso all'utilizzatore prima di procedervi.

➤ DIVIETI E PRESCRIZIONI

Ai sensi del presente Regolamento, limitatamente all'utilizzo degli strumenti informatici aziendali di proprietà e forniti dal Comune:

- Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dall'Amministratore di Sistema per conto del Comune, né viene consentito agli utilizzatori di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre virus informatici, o malware e/o di alterare la funzionalità delle applicazioni software esistenti.
- Salvo preventiva autorizzazione scritta dell'Amministratore di Sistema e/o del Comune, non è consentito all'utilizzatore modificare le caratteristiche impostate sul proprio PC né procedere ad installare/connettere dispositivi di memorizzazione, comunicazione o altro che non siano stati

forniti dal Comune (chiavette USB, masterizzatori, CD/DVD, hard disk esterni). In ogni caso, l'utilizzatore deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente l'Amministratore di Sistema nel caso in cui siano rilevati virus e adottando quanto previsto *infra* relativamente alle procedure di protezione antivirus.

- Tutti i dispositivi di memorizzazione (dischetti, CD e DVD riscrivibili, supporti USB, ecc.), forniti dal Comune contenenti dati personali nonché informazioni costituenti *know-how* aziendale, devono essere trattati con particolare cautela, onde evitare che il loro contenuto possa essere distrutto, perduto, modificato, divulgato in assenza di specifica autorizzazione scritta. L'utilizzatore resta, in ogni caso, responsabile della custodia dei supporti e dei dati del Comune in essi contenuti; in particolare, gli eventuali supporti magnetici contenenti particolari categorie di dati ex art. 9 del GDPR, devono essere custoditi dagli utilizzatori in armadi/scrivanie dotate di chiusura a chiave. Esaurita la finalità/cessata la necessità per cui i dispositivi di memorizzazione sono stati affidati all'utilizzatore, quest'ultimo dovrà consegnarli alla direzione del Comune che provvederà, se del caso, alle operazioni di cancellazione dei dati ivi contenuti, secondo le procedure descritte nella relativa policy, al fine di predisporli per un nuovo utilizzo ed impedire il recupero dei dati precedentemente contenuti.
- Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo. In ogni caso, lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso: pertanto, nei casi in cui non sia possibile o opportuno spegnere il PC, deve essere disconnesso il profilo dell'utente, con obbligo di reintrodurre la password per l'accesso.

GESTIONE E ASSEGNAZIONE DELLE CREDENZIALI DI AUTENTICAZIONE

Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dall'Amministratore di Sistema e/o dalla direzione del Comune, previa espressa indicazione dell'ambito nel quale verrà inserito ed andrà ad operare il nuovo utilizzatore.

Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utilizzatore (User Id), dall'Amministratore di Sistema e/o dalla direzione del Comune, associato ad una parola chiave (password) riservata che dovrà essere custodita dall'operatore con la massima diligenza e non divulgata. Non è pertanto consentito scrivere la password su carta ed esporla a soggetti terzi.

Inoltre:

- Non è consentita l'attivazione della password di accensione (*bios*), senza preventiva autorizzazione scritta del Comune.
- La parola chiave, formata da lettere (maiuscole o minuscole) e numeri, anche in combinazione fra loro, deve essere composta da almeno 8 (OTTO) caratteri, e non deve contenere riferimenti agevolmente riconducibili all'utilizzatore.
- Il sistema ricorda le password per cui non si può ripetere la stessa al momento del cambio della medesima.
- Il numero di tentativi errati ammessi di inserimento password è di 3 volte.
- Il Comune procederà automaticamente al reset della parola chiave ogni 3 mesi.
- In occasione del primo utilizzo della parola chiave, ovvero in occasione dei successivi reset della stessa, l'utilizzatore personalmente procederà alla modifica della parola chiave di default fornita dal Comune.
- Tutti i PC, salvo quelli in uso ad utenti a cui sono stati accordati i privilegi di amministrazione della propria macchina, sono impostati per bloccarsi dopo 15 minuti di inattività. Gli utilizzatori devono bloccare i loro computer quando si allontanano dalla scrivania, sia per motivi di sicurezza delle reti, che per la tutela dei dati personali.

Soggetto preposto alla custodia delle credenziali di autenticazione è l'Amministratore di Sistema del Comune, nella persona di TRAPANESE ROMEO.

UTILIZZO DI DISPOSITIVI ELETTRONICI PORTATILI E BYOD

Tutti i dispositivi elettronici portatili dati in dotazione agli utilizzatori, ove conferiti, sono di proprietà del Comune e devono essere trattati, utilizzati e tutelati con la massima diligenza. Tali dispositivi, come meglio individuati nel prosieguo, costituiscono strumenti per rendere la prestazione lavorativa ex art. 4 comma 2 L. 300/700: ne viene concesso l'uso esclusivamente per lo svolgimento delle attività lavorative, non essendo quindi consentiti utilizzi a carattere personale/privato, o comunque non strettamente inerenti le attività lavorative, a meno che non siano stati esplicitamente autorizzati in forma scritta e in conformità delle istruzioni al riguardo impartite dall'Amministratore di sistema e/o dal Comune.

Tra i dispositivi in questione vanno annoverati, indipendentemente dal fatto che l'utilizzatore abbia o meno la possibilità di accedere alla rete Intranet o di condividere documenti, dati e materiali ivi conservati e/o trattati:

- PC portatili (Laptop)
- Tablet
- Telefoni cellulari/Smartphone

Qualora l'utilizzatore danneggi il dispositivo aziendale, lo smarrisca, ne subisca il furto o riscontri malfunzionamenti nell'utilizzo, dovrà informare tempestivamente, e comunque entro e non oltre 2 ore dalla scoperta, il Comune, che adotterà le misure necessarie per la tutela dei dati personali e aziendali ivi contenuti.

Questi dispositivi consentono agli utilizzatori la possibilità di usufruire di servizi di posta elettronica, contatti e calendari standard nonché applicazioni aziendali in esclusiva conformità con le esigenze aziendali.

Al fine della tutela dei dati personali e del patrimonio aziendale, tutti i dispositivi elettronici portatili aziendali sono dotati di password di protezione. Gli utilizzatori sono tenuti a conservare la propria password e a non divulgarla a nessuno. Se l'utilizzatore dimentica la password, dovrà comunicarlo al Comune per procedere al reset e reimpostazione della password.

Non è consentito l'uso di dispositivi BYOD.

USO DELLA POSTA ELETTRONICA

La casella di posta elettronica assegnata all'utilizzatore è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono, quindi, responsabili del corretto utilizzo delle stesse.

È fatto divieto di utilizzare le caselle di posta elettronica aziendali per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'utilizzatore non potrà utilizzare la posta elettronica per:

- L'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es. mp3) non legati all'attività lavorativa.
- L'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list.
- La partecipazione a catene telematiche (o c.d. "di Sant'Antonio"). Se si dovessero peraltro ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al Comune. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.

La casella di posta elettronica deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

In caso di cessazione del rapporto di lavoro, il singolo dipendente/collaboratore è tenuto ad eliminare dalle proprie cartelle tutti i messaggi di posta elettronica ed i documenti eventualmente non pertinenti

l'attività aziendale e non utili alle esigenze del Comune, mantenendo integra, invece, tutta la corrispondenza e documentazione inerente alla attività lavorativa. Resta inteso che, di conseguenza, la documentazione presente nel profilo del singolo utilizzatore che cessa il rapporto di lavoro verrà considerata presuntivamente dal Comune quale corrispondenza e documentazione lavorativa e non personale.

È obbligatorio porre la massima attenzione nell'aprire gli allegati (*files attachments*) di posta elettronica prima del loro utilizzo e non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti.

In caso di assenze programmate (ad es. per ferie o attività di lavoro fuori sede dell'assegnatario della casella) al fine di garantire la funzionalità del servizio di posta elettronica dal Comune e di ridurre al minimo l'accesso ai dati, nel rispetto del principio di necessità e di proporzionalità, il sistema, potrà inviare automaticamente messaggi di risposta contenenti le coordinate di posta elettronica di un altro soggetto o altre utili modalità di contatto della struttura.

In tal caso, la funzionalità deve essere attivata e disattivata dall'utente.

In caso di assenza non programmata (ad es. per malattia) la procedura - qualora non possa essere attivata dall'utilizzatore avvalendosi del servizio webmail entro due giorni - potrà venire attivata, su richiesta della direzione del Comune, dall'Amministratore di Sistema.

Sarà comunque consentito al superiore gerarchico dell'utilizzatore o, comunque, sentito l'utente titolare della casella di posta elettronica, a persona individuata dal Comune, di accedere alla casella di posta elettronica dell'utilizzatore per ogni ipotesi in cui si renda necessario, al fine di garantire la continuità aziendale e la sicurezza delle reti.

Al fine di ribadire agli interlocutori la titolarità esclusivamente in capo al Comune della casella di posta elettronica, si suggerisce di aggiungere in coda ad ogni messaggio e-mail, indirizzato a destinatari esterni, un avvertimento standardizzato, nel quale sia dichiarata la natura non personale dei messaggi stessi e precisando che, pertanto, il soggetto specificatamente individuato dal Comune potrà accedere al contenuto del messaggio inviato alla stessa casella.

La casella di posta elettronica viene cancellata al momento della conclusione del rapporto di lavoro che ne giustificava l'assegnazione. Il Comune si riserva, tuttavia, di valutare la necessità di mantenere attiva in ricezione la casella per un periodo non superiore a 3 mesi al fine di garantire la continuità dal Comune. In tal caso:

- avrà accesso alla casella esclusivamente la direzione o l'Amministratore di Sistema del Comune, il quale ultimo provvederà anche agli adempimenti necessari alla chiusura definitiva dell'account;
- verranno inviate e-mail ai mittenti con indicazione della diversa casella di posta elettronica a cui trasmettere i messaggi;
- viene escluso, comunque, l'invio di messaggi da tale casella di posta diversi da quelli di cui al punto precedente.

Nel caso in cui venisse assegnato all'utilizzatore anche la gestione di più indirizzi di posta elettronica certificata di cui il Comune si fosse dotata, tale utilizzatore dovrà attenersi alle disposizioni del presente regolamento, in quanto applicabili.

UTILIZZO DELLA RETE INTERNET

Il PC assegnato al singolo utilizzatore ed abilitato alla navigazione in Internet costituisce uno strumento del Comune utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa.

È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa.

In questo senso, a titolo puramente esemplificativo, l'utilizzatore non potrà utilizzare Internet per:

- l'upload o il download di software anche gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web o *http*, se non strettamente attinenti all'attività lavorativa e previa verifica dell'attendibilità dei siti in questione;
- l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dalla direzione del Comune e comunque nel rispetto delle normali procedure di acquisto;
- ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- la partecipazione a forum non professionali, l'iscrizione con account ed indirizzi di posta elettronica aziendale e la partecipazione personale a social network, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati;
- l'accesso, tramite Internet, a caselle webmail di posta elettronica personale durante l'orario di lavoro. In ogni caso, l'utilizzatore dovrà comunque porre la massima attenzione nell'aprire gli allegati di posta elettronica prima del loro utilizzo.

L'utilizzo della rete Wi-Fi presente è limitato agli utenti interni autorizzati e agli utenti esterni che, con credenziali d'accesso assegnate dalla direzione del Comune/Amministratore di Sistema, avranno accesso a una rete di tipo "*guest*" configurata in modo da consentire la navigazione, ma non l'accesso alla LAN del Comune

PROTEZIONE ANTIVIRUS

Gli strumenti informatici di proprietà del Comune sono protetti da software antivirus aggiornato regolarmente e frequentemente. Ogni utilizzatore deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico dal Comune mediante virus o mediante ogni altro software aggressivo.

Ogni dispositivo di memorizzazione di provenienza esterna dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato alla direzione del Comune

Nel caso il software antivirus rilevi la presenza di un virus e l'utilizzatore riscontri una perdita/modifica/sottrazione/distruzione di dati, lo stesso dovrà:

- Segnalare prontamente, e comunque entro e non oltre 60 minuti, l'accaduto al Servizio CED, nella persona di TRAPANESE ROMEO, e coadiuvare la medesima a redigere un report con le circostanze d'incidente a lui note.
- In caso di assenza di TRAPANESE ROMEO, e qualora non risulti possibile comunicargli l'accaduto in tempi estremamente rapidi, e comunque non oltre le 2 ore, rivolgersi al sostituto ed all'uopo autorizzato, individuato nella persona di QUIRICO MARINELLA.

In caso di Data Breach, l'incidente verrà gestito secondo le disposizioni impartite dalla specifica policy aziendale "*Data Breach & Incident Response*" adottata dall'azienda

PARTECIPAZIONE A *SOCIAL MEDIA*

L'eventuale utilizzo a fini promozionali e commerciali dei *social media* - quali Facebook™, Twitter™, LinkedIn™, dei blog e dei forum, anche professionali - verrà gestito ed organizzato esclusivamente dal Comune attraverso specifiche direttive ed istruzioni operative al personale/collaboratori a ciò espressamente addetto, rimanendo escluse iniziative individuali da parte dei singoli utenti.

Fermo restando il pieno ed inderogabile diritto della persona alla libertà di espressione ed al libero scambio di idee ed opinioni, Il Comune ritiene comunque opportuno indicare agli utenti alcune regole comportamentali, al fine di tutelare tanto la propria immagine ed il proprio patrimonio, anche immateriale, quanto i propri collaboratori, i propri clienti e fornitori, gli altri partners, oltre che gli stessi utilizzatori dei social media, fermo restando che viene vietata la partecipazione agli stessi social media a titolo personale durante l'orario di lavoro. La policy qui dettata deve coinvolgere gli utilizzatori, sia che utilizzino dispositivi

messi a disposizione dal Comune, sia che utilizzino propri dispositivi, sia che partecipino ai social media a titolo personale, sia che lo facciano per finalità professionali, come dipendenti o collaboratori della stessa Il Comune

La condivisione dei contenuti nei social media deve sempre rispettare e garantire la segretezza sulle informazioni del Comune e dei dati personali considerati dal Comune riservate ed in genere, a titolo esemplificativo e non esaustivo, sulle informazioni finanziarie ed economiche, commerciali, sui clienti, sui fornitori ed altri partners del Comune

Inoltre, ogni comunicazione e divulgazione di contenuti dovrà essere effettuata nel pieno rispetto dei diritti di proprietà industriale e dei diritti d'autore, sia di terzi che del Comune; l'utente, nelle proprie comunicazioni, non potrà, quindi, inserire marchi od altri segni distintivi del Comune, né potrà pubblicare disegni, modelli od altro connesso ai citati diritti. Ogni deroga a quanto sopra disposto potrà peraltro avvenire solo previa specifica preventiva autorizzazione della direzione del Comune

L'utilizzatore deve garantire la tutela della privacy delle persone; di conseguenza, non potrà comunicare o diffondere dati personali (quali dati anagrafici, immagini, video, suoni e voci, ecc.) di colleghi e in genere di collaboratori del Comune, se non con il preventivo personale consenso scritto di questi, e comunque non potrà postare nel social media immagini, video, suoni e voci registrati all'interno del luogo di lavoro, se non con il preventivo consenso scritto della direzione del Comune

L'utilizzatore risponde personalmente dei propri comportamenti, e deve astenersi dal porre in essere, nei confronti in genere di terzi e specificatamente verso il Comune, i colleghi, i clienti ed i fornitori, attività che possano essere penalmente o civilmente rilevanti; a titolo esemplificativo, sono quindi vietati comportamenti ingiuriosi, diffamatori e denigratori, discriminatori o che configurano molestie. In tal senso, è vivamente auspicato da parte di tutti un comportamento civile e sobrio, in particolar modo in qualunque occasione in cui l'espressione o il contesto in cui essa avviene possa essere collegata all'ambito lavorativo.

Infine, in via generale ed ove non autorizzato in senso diverso dalla direzione del Comune, l'utente, nell'utilizzo dei social network, esprimerà unicamente le proprie opinioni personali; pertanto, ove necessario od opportuno per la possibile connessione con il Comune, in particolare in forum professionali, l'utilizzatore dovrà precisare che le opinioni espresse sono esclusivamente personali e non riconducibili a Il Comune.

DISCIPLINA DELLE ATTIVITA' DI CONTROLLO SUGLI STRUMENTI INFORMATICI E TELEMATICI

Al fine di tutelare la sicurezza della rete, il patrimonio aziendale del Comune ed al fine di garantire la protezione dei sistemi e dei dati personali trattati dal Comune da condotte, ancorché accidentali, idonee a configurare ipotesi di reato o illeciti commessi con modalità informatiche o telematiche, nel rispetto del principio di necessità, proporzionalità e non eccedenza, Il Comune potrà esercitare attività di verifica delle attività di navigazione o di fruizione dei servizi, , limitatamente all'area di sistema deputata alla sfera professionale dell'utilizzatore, ed in ogni caso sotto la supervisione contestuale dello stesso.

Gli strumenti informatici e telematici disciplinati dal presente Regolamento costituiscono tutti strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa, ai sensi e per gli effetti dell'art. 4, comma secondo, della Legge n. 300/1970 come modificato dalla D.lgs. 150/2015; conseguentemente, le informazioni raccolte possono essere utilizzate a tutti i fini connessi al rapporto di lavoro, essendone stata data informazione ai lavoratori sulle modalità di uso degli strumenti stessi, sugli interventi che potranno venir compiuti nel sistema informatico aziendale ovvero nel singolo strumento e sui conseguenti sistemi di controllo che potessero venir eventualmente compiuti, fermo restando il rispetto della normativa in materia di protezione dei dati personali.

Viene, infine, precisato che non sono installati o configurati sui sistemi informatici in uso agli utenti apparati hardware o strumenti software aventi come scopo il controllo a distanza dell'attività dei lavoratori; peraltro, laddove l'adozione di tali apparati risultasse necessaria per finalità altre, es. esigenze organizzative e/o produttive, di sicurezza del lavoro e/o di tutela del patrimonio aziendale, Il Comune

provvederà conformemente a quanto disposto dall'art. 4, comma primo, della Legge n. 300/1970 come modificato dal D.lgs. 150/2015, dandone anche opportuna informazione agli utenti stessi.

Gli eventuali controlli, compiuti dall'Amministratore di Sistema ai sensi del precedente punto, potranno avvenire mediante un sistema di controllo dei contenuti delle comunicazioni elettroniche e dei relativi file allegati, anche mediante "*files di log*".

I suddetti controlli, anche sui files di log, vengono svolti a campione, in maniera non continuativa e per le esclusive finalità sopra elencate.

In caso di anomalie, l'Amministratore di Sistema potrà effettuare controlli anonimi che si concluderanno con avvisi generalizzati diretti ai dipendenti/collaboratori dell'area in cui è stata rilevata l'anomalia, nei quali si evidenzierà l'utilizzo irregolare degli strumenti informatici e si inviteranno gli stessi ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

Controlli su base più ristretta o anche individuale potranno essere compiuti solo in caso di successive ulteriori anomalie.

Qualora dai suddetti controlli venga rilevata una anomalia tale da configurare, ancorché astrattamente, una condotta civilmente e/o penalmente rilevante, Il Comune si riserva, ai fini di esercizio dei propri diritti difensivi ex art. 4 comma 3 L. 300/1970 come modificato dal D.lgs. 150/2015, ed in ottemperanza ai provvedimenti ed autorizzazioni generali dell'Autorità Garante per la protezione dei dati personali, di conservare l'evidenza rilevata, anche mediante acquisizione forense, per il tempo necessario all'esercizio dei predetti diritti.

In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

ACCESSO AI DATI TRATTATI DALL'UTILIZZATORE

Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, software etc.) o per finalità di controllo e programmazione dei costi aziendali (ad esempio, verifica costi di connessione ad Internet, traffico telefonico, ecc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà della direzione del Comune, per il tramite dell'Amministratore di Sistema, accedere direttamente, nel rispetto della normativa sulla privacy e delle procedure di cui ai precedenti punti, a tutti gli strumenti informatici e ai documenti aziendali ivi contenuti.

Con riferimento all'eventuale utilizzo di sistemi BYOD, l'accesso agli strumenti informatici e ai documenti aziendali ivi contenuti è limitato all'area di sistema deputata alla sfera professionale dell'utilizzatore, ed in ogni caso sotto la supervisione dello stesso.

OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY

È obbligatorio per tutti gli utilizzatori attenersi alle disposizioni in materia di protezione dei dati personali adottate secondo i principi e i limiti individuati dal Regolamento (UE) 2016/679 (c.d. GDPR), come indicato nelle lettere d'autorizzazione per ciascun utilizzatore.

SANZIONI

È fatto obbligo a tutti gli utilizzatori di osservare le disposizioni portate a conoscenza con il presente Regolamento. Il mancato rispetto o la violazione delle regole sopra ricordate, anche a seguito di controlli a campione come sopra definiti e considerata la natura della violazione/irregolarità rilevata, è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dal vigente CCNL ed ai sensi dell'art. 4 L. 300/70 come modificata dal D.lgs. 150/2015, e nei confronti dei collaboratori e consulenti, verificata la gravità della violazione contestata, con la risoluzione od il recesso dal contratto ad essi relativo nonché con tutte le azioni civili e penali consentite dalle leggi applicabili.

AGGIORNAMENTO E REVISIONE

Il presente Regolamento è soggetto ad eventuale aggiornamento annuale, salve specifiche esigenze determinate da modifiche/aggiornamenti normativi e regolamentari.

ENTRATA IN VIGORE DEL REGOLAMENTO E PUBBLICITÀ

Con l'entrata in vigore del presente Regolamento, tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi superate e sostituite dalle disposizioni previste dalla presente disciplina.

Copia del presente Regolamento verrà resa disponibile per la visualizzazione nella cartella comune sul server del Comune, nell'apposita cartella "\\SERVERSQL\\REGOLAMENTO STRUMENTI INFORMATICI", a disposizione di tutti gli utilizzatori, debitamente avvertiti via email della disponibilità dello stesso nella predetta cartella condivisa.

Si invita a renderlo noto e richiederne l'applicazione, eventualmente richiamandolo, ove possibile, nella relativa documentazione contrattuale, anche a collaboratori, consulenti, od altri incaricati esterni che venissero autorizzati a far uso di strumenti informatici o telefonici di proprietà del Comune, ad accedere mediante dispositivi propri (in tal caso si parla di BYOD) alla rete informatica dell'Ente e/o ad informazioni ivi conservate e trattate.