COMUNE DI RESANA
Provincia di Treviso

REGOLAMENTO PER L'UTILIZZO DEI SISTEMI INFORMATICI

Premessa

Il presente Regolamento intende fornire a dipendenti, collaboratori e altri soggetti a cui è concesso l'uso delle risorse informatiche del Comune, da qui in poi denominati anche incaricati o utenti, le indicazioni per una corretta e adeguata gestione delle informazioni, in particolare attraverso l'uso di sistemi, applicazioni e strumenti informatici dell'Ente.

Si specifica che tutti gli strumenti utilizzati dal lavoratore, intendendo con ciò PC, notebook, risorse, e-mail ed altri strumenti con relativi software e applicativi (di seguito più semplicemente "Strumenti"), sono messi a disposizione dall'Ente per rendere la prestazione lavorativa. Gli Strumenti, nonché le relative reti a cui è possibile accedere tramite gli stessi, sono domicilio informatico dell'Ente.

I dati personali e le altre informazioni dell'Utente registrati negli Strumenti o che si possono eventualmente raccogliere tramite il loro uso, sono utilizzati per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio. Per tutela del patrimonio si intende altresì la sicurezza informatica e la tutela del sistema informatico. Tali informazioni sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, visto che il presente Regolamento costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal Regolamento Europeo 679/16 sulla 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.

Indice

1 Oggetto e finalità

Il presente Regolamento è redatto:

- Alla luce della Legge 20.5.1970, n. 300, recante "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento";
- In attuazione del Regolamento Europeo 679/16 sulla protezione dei dati personali (d'ora in avanti Reg. 679/16 o GDPR);
- Ai sensi delle "Linee guida del Garante per posta elettronica e internet" in Gazzetta Ufficiale n. 58 del 10 marzo 2007;
- Alla luce dell'articolo 23 del D.Lgs. n. 151/2015 (c.d. Jobs Act) che modifica e rimodula la fattispecie integrante il divieto dei controlli a distanza, nella consapevolezza di dover tener conto, nell'attuale contesto produttivo, oltre agli impianti audiovisivi, anche degli altri strumenti *«dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori»* e di quelli *«utilizzati dal lavoratore per rendere la prestazione lavorativa».*

La finalità è quella di promuovere una corretta "cultura informatica" affinché l'utilizzo degli Strumenti informatici e telematici forniti dall'Ente, quali la posta elettronica, internet e i personal computer con i relativi software, sia conforme alle finalità e nel pieno rispetto della legge. Si vuole fornire a tutti gli utenti le indicazioni necessarie con l'obiettivo principale di evitare il verificarsi di qualsiasi abuso o uso non conforme, muovendo dalla convinzione che la prevenzione dei problemi sia preferibile rispetto alla loro successiva correzione.

2 Principi generali e di riservatezza nelle comunicazioni

2.1 I principi che sono a fondamento del presente Regolamento sono gli stessi espressi nel GDPR, e, precisamente:

a) **Il principio di necessità**, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite (art. 5 e 6 del Reg. 679/16);

b) **Il principio di correttezza**, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note agli utenti. Le tecnologie dell'informazione (in modo più marcato rispetto ad apparecchiature tradizionali) permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa. Ciò, all'insaputa o senza la piena consapevolezza degli utenti, considerate anche le potenziali applicazioni di regola non adeguatamente conosciute dagli interessati;

c) **I trattamenti devono essere effettuati per finalità determinate, esplicite e legittime** (art.5 commi 1 e 2), osservando il principio di pertinenza e non eccedenza. Il datore di lavoro deve trattare i dati "nella misura meno invasiva possibile"; le attività di monitoraggio devono essere svolte solo da soggetti preposti ed essere "mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza".

2.2 È riconosciuto al datore di lavoro di potere svolgere attività di monitoraggio, che nella fattispecie saranno svolte solo dall'Amministratore di Sistema o dal personale delegato dall'Amministratore di Sistema, sempre nel rispetto della succitata normativa.

2.3 L'utente si attiene alle seguenti regole di trattamento:

a) È vietato comunicare a soggetti non specificatamente autorizzati i dati personali comuni, sensibili, giudiziari, sanitari o altri dati, elementi e informazioni dei quali l'incaricato viene a conoscenza nell'esercizio delle proprie funzioni e mansioni all'interno dell'Ente. In caso di

dubbio, è necessario accertarsi che il soggetto cui devono essere comunicati i dati sia o meno autorizzato a riceverli, mediante richiesta preventiva al proprio Responsabile di area/funzione.

b) È vietata l'estrazione di originali e/o copie cartacee ed informatiche per uso personale di documenti, manuali, fascicoli, lettere, data base e quant'altro.

c) È vietato lasciare incustoditi documenti, lettere, fascicoli, appunti e quant'altro possa contenere dati personali e/o informazioni quando l'incaricato si allontana dalla postazione di lavoro. È vietato lasciare sulla postazione di lavoro (scrivania, bancone ecc.) materiali che non siano inerenti la pratica che si sta trattando in quel momento. Ciò vale soprattutto nel caso di lavoratori con mansioni di front office e di ricezione di Clienti / Fornitori o colleghi di lavoro.

d) Per le riunioni e gli incontri con clienti, fornitori, consulenti e collaboratori dell'Ente è necessario utilizzare le eventuali zone o sale dedicate.

3 Tutela del lavoratore

3.1 Alla luce dell'art. 4, comma 1, L.n. 300/1970, la regolamentazione della materia indicata nell'art. 1 del presente Regolamento, non è finalizzata all'esercizio di un controllo a distanza dei lavoratori da parte del datore di lavoro ma solo a permettere a quest'ultimo di utilizzare sistemi informativi per fare fronte ad esigenze produttive od organizzative e di sicurezza nel trattamento dei dati personali.

3.2 È garantito al singolo lavoratore il controllo sui propri dati personali secondo quanto previsto dagli articoli 15-16-17-18-20-21-77 del Reg. 679/16.

4 Campo di applicazione

4.1 Il presente regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o di livello, nonché a tutti i collaboratori dell'Ente a prescindere dal rapporto contrattuale con la stessa intrattenuto ed in generale a tutti gli individui a cui è concesso l'uso delle risorse informatiche del Comune.

4.2 Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni individuo in possesso di specifiche credenziali di autenticazione al sistema informatico comunale. Tale figura potrà anche venir indicata come "incaricato del trattamento".

5 Gestione, assegnazione e revoca delle credenziali di accesso

5.1 Le credenziali di autenticazione per l'accesso alle risorse informatiche vengono assegnate dall'Amministratore di Sistema, previa formale richiesta del Responsabile del Servizio nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente. Nel caso di collaboratori esterni la richiesta dovrà essere inoltrata direttamente dal Responsabile del Servizio con il quale l'utente si coordina nell'espletamento del proprio incarico. La richiesta di attivazione delle credenziali dovrà essere completa di generalità dell'utente ed elenco dei sistemi informativi per i quali deve essere abilitato l'accesso. Ogni successiva variazione delle abilitazioni di accesso ai sistemi informativi dovrà essere richiesta formalmente all'Amministratore di Sistema dal Responsabile di riferimento.

5.2 Le credenziali di autenticazioni consistono in un codice per l'identificazione dell'utente (altresì nominati username, nome utente o user id), assegnato dall'Amministratore di Sistema, ed una relativa password. La password è personale e riservata e dovrà essere conservata e custodita dall'incaricato con la massima diligenza senza divulgarla.

5.3 La password deve essere di adeguata robustezza: deve essere composta da almeno 8 caratteri, formata da lettere maiuscole e minuscole e/o numeri. Non deve contenere riferimenti agevolmente riconducibili all'utente (username, nomi o date relative alla persona o ad un familiare).

5.4 È necessario procedere alla modifica della password a cura dell'utente al primo accesso e, successivamente, almeno ogni sei mesi. Nel caso in cui l'utente svolga mansioni che, in astratto, possano comportare il trattamento di dati personali sensibili, è obbligatorio il cambio password almeno ogni tre mesi.

5.5 Nel caso di cessazione del rapporto di lavoro o dell'incarico con l'utente, il Responsabile del Servizio di riferimento dovrà comunicare formalmente e preventivamente all'Amministratore di Sistema la data effettiva a partire dalla quale le credenziali saranno disabilitate.

PASSWORD

Il più semplice metodo per l'accesso illecito a un sistema consiste nell'indovinare la password dell'utente legittimo. In molti casi sono stati procurati seri danni al sistema informativo a causa di un accesso protetto da password "deboli". La scelta di password "forti" è quindi parte essenziale della sicurezza informatica.

COSA NON FARE

1. NON dite a nessuno la Vostra password. Ricordate che lo scopo principale per cui usate una password è assicurare che nessun altro possa utilizzare le Vostre risorse e che soprattutto possa farlo a Vostro nome;
2. NON scrivete la password da nessuna parte che possa essere letta facilmente, soprattutto vicino al computer;
3. Quando immettete la password NON fate guardare a nessuno quello che state battendo sulla tastiera;
4. NON scegliete come password delle parole comuni, anche il lingua straniera: sono facilmente individuabili;
5. NON usate il Vostro nome utente: è la password più semplice da indovinare;
6. NON usate password che possano in qualche modo essere legate a Voi come, ad esempio, il Vostro nome, quello di Vostra moglie/marito, dei figli, del cane, date di nascita, numeri di telefono etc.

COSA FARE

1. Cambiare la password a intervalli regolari: a prescindere dall'esistenza di un sistema automatico di richiesta di aggiornamento password, queste devono essere sostituite almeno nei tempi indicati dalla normativa;
2. Usare sempre password lunghe almeno otto caratteri con un misto di lettere maiuscole e minuscole, numeri e caratteri speciali;
3. Cambiare immediatamente una password non appena si abbia il dubbio che sia diventata poco "sicura";
4. Utilizzate password distinte per sistemi con diverso grado di sensibilità. In alcuni casi la password viaggiano in chiaro sulla rete e possono essere quindi intercettate, per cui, oltre a cambiarla spesso, è importante che sia diversa per quella usata su sistemi "sicuri".

Le migliori password sono quelle facili da ricordare ma, allo stesso tempo, difficili da indovinare, come quelle che si possono ottenere comprimendo frasi lunghe. La frase "C'era una volta una gatta!" può ad esempio servire per ricordare la password "Cr1Vlt1Gtt!".

6 Utilizzo della rete LAN

6.1 Per l'accesso alle risorse informatiche dell'Ente attraverso la rete locale, ciascun utente deve essere in possesso di credenziali di autenticazione secondo l'art. 5.

6.2 È assolutamente proibito accedere alla rete ed ai sistemi informativi utilizzando credenziali di altre persone.

6.3 L'accesso alla rete garantisce all'utente la disponibilità di condivisioni di rete (cartelle su server) nelle quali vanno inseriti e salvati i file di lavoro, organizzati per area/ufficio o per diversi criteri o per obiettivi specifici di lavoro. Ciascun utente, poi, dispone di un'area riservata e personale. Tutte le cartelle di rete, siano esse condivise o personali, possono ospitare esclusivamente contenuti professionali o istituzionali. Pertanto è vietato il salvataggio sui server dell'Ente, ovvero sugli Strumenti, di documenti non inerenti l'attività lavorativa o istituzionale, quali a titolo esemplificativo documenti, fotografie, video, musica, pratiche personali, sms, mail personali, film e quant'altro. Eventuale materiale personale rilevato dall'Amministratore di Sistema a seguito di interventi di sicurezza informatica ovvero di manutenzione/aggiornamento su server ed anche su Strumenti viene

rimosso secondo le regole previste nel successivo punto 12 del presente Regolamento, ferma ogni ulteriore responsabilità civile, penale e disciplinare. Tutte le risorse di memorizzazione, diverse da quelle citate al punto precedente, non sono sottoposte al controllo regolare dell'Amministratore di Sistema e possono non essere oggetto di backup periodici. A titolo di esempio e non esaustivo si citano: il disco C o altri dischi locali dei singoli PC o la cartella "Desktop" dell'utente, gli eventuali dispositivi di memorizzazione locali o di disponibilità personale come Hard disk portatili o NAS ad uso esclusivo. Tutte queste aree di memorizzazione non devono ospitare dati di interesse, poiché non sono garantite la sicurezza e la protezione contro la eventuale perdita di dati. Pertanto la responsabilità dei salvataggi dei dati ivi contenuti è a carico del singolo utente.

6.4 Senza il consenso del Responsabile del Servizio, è vietato trasferire documenti elettronici dai sistemi informativi e Strumenti dell'Ente a dispositivi esterni (hard disk, chiavette, CD, DVD e altri supporti).

6.5 Senza il consenso del Responsabile del Servizio è vietato salvare documenti elettronici dell'Ente (ad esempio pervenuti via mail o conservati sul Server o sullo Strumento in dotazione) su repository esterne (quali ad esempio Dropbox, Google Drive, Microsoft OneDrive, ecc.) ovvero inviandoli a terzi via posta elettronica o con altri sistemi.

6.6 Con regolare periodicità (almeno una volta al mese), ciascun utente provvede alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

6.7 L'Ente può mettere a disposizione dei propri utenti la possibilità di accedere alle proprie risorse informatiche anche dall'esterno mediante rete VPN (Virtual Private Network), un canale privato e criptato verso la rete interna, oppure mediate sistemi di desktop remoto opportunamente securizzati e protetti. L'accesso dall'esterno viene concesso a consulenti, professionisti, tecnici e fornitori che nell'ambito di un rapporto contrattuale con l'Ente necessitino di accedere a determinate risorse informatiche; viene concesso, altresì, a dipendenti e funzionari dell'Ente che necessitino di svolgere compiti specifici, pur non essendo presenti in sede. Le richieste di abilitazione all'accesso alle risorse informatiche dall'esterno dovranno seguire le prescrizioni del punto 5.

6.8 All'interno delle sedi lavorative può essere resa disponibile anche una rete senza fili, c.d. "Wi-Fi". Tali reti consentono l'accesso alle risorse e ad internet per i dispositivi non connessi alla rete LAN mediante cavo. L'accesso mediante rete Wi-Fi viene concesso a consulenti, professionisti, tecnici e fornitori che nell'ambito di un rapporto contrattuale con l'Ente necessitino di accedere a determinate risorse informatiche. Viene concesso, altresì, a dipendenti e funzionari dell'Ente che necessitino di svolgere compiti specifici che non possono essere svolti dalle postazioni fisse. L'impostazione della connessione Wi-Fi sarà effettuata dall'Amministratore di Sistema. Questa rete Wi-Fi è di tipo privato e non va confusa con l'eventuale presenza di hot spot Wi-Fi pubblici che danno accesso internet al pubblico in modo completamento distinto dall'infrastruttura informatica comunale e gestiti da Internet Service Provider (ISP).

6.9 L'Amministratore di Sistema si riserva la facoltà di negare o interrompere l'accesso alla rete mediante dispositivi non adeguatamente protetti e/o aggiornati, che possano costituire una concreta minaccia per la sicurezza informatica.

I log relativi all'uso del File System e della intranet, nonché i file salvati o trattati su Server o Strumenti, sono registrati e possono essere oggetto di controllo da parte del Titolare del trattamento, attraverso l'Amministratore di Sistema, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente.
I controlli possono avvenire secondo le disposizioni previste al successivo punto 12 del presente Regolamento.

Le informazioni così raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Regolamento Europeo 679/16 (GDPR).

7 Utilizzo degli Strumenti elettronici (PC, notebook e altri strumenti con relativi software e applicativi)

7.1 L'utente è consapevole che gli Strumenti forniti sono di proprietà dell'Ente e devono essere utilizzati esclusivamente per rendere la prestazione lavorativa o in relazione al proprio incarico. Ognuno è responsabile dell'utilizzo delle dotazioni informatiche ricevute in assegnazione. Ogni utilizzo non inerente l'attività lavorativa o istituzionale è vietato in quanto può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Ciascun incaricato si deve quindi attenere alle seguenti regole di utilizzo degli Strumenti.

7.2 L'accesso agli Strumenti è protetto da password; per l'accesso devono essere utilizzati Username e password assegnate dall'Amministratore di Sistema (cfr. 5). A tal proposito si rammenta che essi sono strettamente personali e l'utente è tenuto a conservarli nella massima segretezza. Non è consentito l'accesso con credenziali non proprie salvo casi specifici autorizzati dal Responsabile del Servizio.

7.3 Personal Computer, notebook, tablet ed ogni altro dispositivo hardware deve essere custodito con cura da parte degli assegnatari evitando ogni possibile forma di danneggiamento e segnalando tempestivamente all'Amministratore di Sistema ogni malfunzionamento e/o danno rilevato. Non è consentita l'attivazione della password d'accensione (BIOS), senza preventiva autorizzazione da parte dell'Amministratore di Sistema.

7.4 Non è consentito all'utente modificare le caratteristiche hardware e software impostate sugli Strumenti assegnati, salvo preventiva autorizzazione da parte dell'Amministratore di Sistema.

7.5 L'utente è tenuto a scollegarsi dal sistema, o bloccare l'accesso, ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicata la stazione di lavoro (PC) o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima: lasciare un PC 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.

7.6 Le informazioni archiviate sul PC locale non sono sottoposte a processi di backup, salvo casi specifici, e la loro gestione è demandata all'utente.

7.7 L'utente utilizzatore dovrà provvedere a memorizzare sulle condivisioni di rete i dati di rilevanza d'ufficio che possono essere utilizzati anche da altri utenti, evitando di mantenere l'esclusività su di essi.

7.8 L'Amministratore di Sistema può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosa per la sicurezza dei PC, per la rete locale e server, nonché potrà cambiare tutte le impostazioni eventualmente configurate che possano interferire con il corretto funzionamento dei servizi informatici dell'Ente.

7.9 Nel caso vengano richiesti all'utente, è obbligatorio consentire l'installazione degli aggiornamenti di sistema al primo momento disponibile in modo tale da mantenere il PC sempre protetto.

7.10 È vietato utilizzare il PC per l'acquisizione, la duplicazione e/o la trasmissione illegale di opere protette da copyright.

7.11 È vietato l'utilizzo di supporti di memoria (chiavi USB, CD, DVD o altri supporti) per il salvataggio di dati trattati tramite gli Strumenti, salvo che il supporto utilizzato sia stato fornito o autorizzato dall'Amministratore di Sistema. In tale caso, il supporto può essere utilizzato esclusivamente per finalità lavorative.

7.12 È assolutamente vietato connettere al PC qualsiasi periferica non autorizzata preventivamente dall'Amministratore di Sistema.

7.13 È assolutamente vietato connettere alla rete locale qualsiasi dispositivo (PC esterni, router, switch, modem, etc.) non autorizzato preventivamente dall'Amministratore di Sistema.

7.14 Nel caso in cui l'utente dovesse notare comportamenti anomali del PC è tenuto a comunicarlo tempestivamente all'Amministratore di Sistema.

I log relativi all'utilizzo di Strumenti, reperibili nella memoria degli Strumenti stessi ovvero sui Server o sugli apparati di rete, nonché i file con essi trattati sono registrati e possono essere oggetto di controllo da parte del Titolare del trattamento, attraverso l'Amministratore di Sistema, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio.
I controlli possono avvenire secondo le disposizioni previste al successivo punto 12 del presente Regolamento.
Le informazioni così raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Regolamento Europeo 679/16 (GDPR).

8 Utilizzo di internet

Le regole di seguito specificate sono adottate anche ai sensi delle "Linee guida del Garante per posta elettronica e internet" pubblicate in Gazzetta Ufficiale n. 58 del 10 marzo 2007.
Ciascun utente si deve attenere alle seguenti regole di utilizzo della rete Internet e dei relativi servizi.

8.1 È ammessa la sola navigazione in siti considerati correlati con la prestazione lavorativa.

8.2 È vietato compiere azioni che siano potenzialmente in grado di arrecare danno all'Ente, ad esempio, il download o l'upload di file audio e/o video, l'uso di servizi di rete con finalità ludiche o comunque estranee all'attività lavorativa o all'incarico svolto.

8.3 È vietato a chiunque il download di qualunque tipo di software gratuito (freeware), shareware o commerciale prelevato da siti Internet senza, se non espressamente autorizzato dagli Amministratori di Sistema.

8.4 Alle postazioni di lavoro sono applicate policy che impediscono l'accesso a contenuti non appropriati o potenzialmente pericolosi; sono vietate pratiche mirate a bypassare tali filtri. In caso sia necessario accedere a siti che risultano bloccati va fatta apposita motivata richiesta all'Amministratore di Sistema.

8.5 Nel caso in cui, per ragioni di servizio, si necessiti di una navigazione libera dai filtri, è necessario richiedere lo sblocco mediante una mail indirizzata all'Amministratore di Sistema ed in copia al Responsabile di Servizio di riferimento, nella quale siano indicati chiaramente: motivo della richiesta, utente e postazione da cui effettuare la navigazione libera, intervallo di tempo richiesto per completare l'attività. L'utente, nello svolgimento delle proprie attività, deve comunque tenere presente in modo particolare il punto 13 e 14 del presente regolamento. Al termine dell'attività l'Amministratore di Sistema ripristinerà i filtri alla situazione iniziale.

8.6 È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo i casi direttamente autorizzati dal Responsabile di Servizio di riferimento, con il rispetto delle normali procedure di acquisto.

8.7 È assolutamente vietato l'utilizzo di abbonamenti privati per effettuare la connessione a Internet tranne in casi del tutto eccezionali e previa autorizzazione dell'Amministratore di Sistema e del Responsabile di Servizio di riferimento.

8.8 È vietata la partecipazione a Forum, Social Network, chat line, di bacheche elettroniche e registrazioni in guest books anche utilizzando pseudonimi o nicknames, salvo specifica autorizzazione

del Responsabile del Servizio. L'accesso a social network è consentito per attività inerenti all'incarico specificatamente affidato nella gestione dei canali social istituzionali.

8.9 È consentito l'uso di strumenti di messaggistica istantanea, per permettere una efficace e comoda comunicazione tra i colleghi, mediante i soli strumenti autorizzati dall'Amministratore di Sistema. Tali strumenti hanno lo scopo di migliorare la collaborazione tra utenti aggiungendo un ulteriore canale comunicativo rispetto agli spostamenti fisici, alle chiamate telefoniche ed e-mail. È consentito un utilizzo legato esclusivamente a scopi professionali o istituzionale. Anche su tali strumenti di messaggistica istantanea è attivo il monitoraggio e la registrazione dell'attività degli utenti, secondo le disposizioni del punto 13 e 14 del presente regolamento.

8.10 Per motivi tecnici e di buon funzionamento del sistema informatico è buona norma, salvo comprovata necessità, non accedere a risorse web che impegnino in modo rilevante banda, come a titolo esemplificativo: filmati (tratti da YouTube, siti di informazione, siti di streaming ecc.) o web radio, in quanto possono limitare e/o compromettere l'uso della rete agli altri utenti.

Si informa che l'Ente, per il tramite dell'Amministratore di Sistema, non effettua la memorizzazione sistematica delle pagine web visualizzate dal singolo Utente, né controlla con sistemi automatici i dati di navigazione dello stesso.
Si informa tuttavia che al fine di garantire il Servizio Internet e la sicurezza dei sistemi informativi, nonché per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio, l'Ente registra per 180 giorni i dati di navigazione (file di log riferiti al traffico web) con modalità inizialmente volte a precludere l'immediata e diretta identificazione di Utenti, mediante opportune aggregazioni.
Solo in casi eccezionali e di comprovata urgenza rispetto alle finalità sopra descritte, l'Ente potrà trattare i dati di navigazione riferendoli specificatamente ad un singolo nome utente. In tali casi i controlli avverranno nelle forme indicate al successivo punto 12 del presente Regolamento. Le informazioni così raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Regolamento Europeo 679/16 (GDPR).

9 Utilizzo della posta elettronica

Le regole di seguito specificate sono adottate anche ai sensi delle "Linee guida del Garante per posta elettronica e internet" pubblicate in Gazzetta Ufficiale n. 58 del 10 marzo 2007.
Ciascun utente si deve attenere alle seguenti regole di utilizzo dell'indirizzo della posta elettronica.

9.1 Ad ogni utente viene fornito un account e-mail nominativo, generalmente coerente con il modello nome.cognome*@comune.resana.tv.it.* L'utilizzo dell'e-mail deve essere limitato esclusivamente a scopi lavorativi o istituzionali, è vietato l'utilizzo per scopi privato. L'utente a cui è assegnata una casella di posta elettronica è responsabile del corretto utilizzo della stessa.

9.2 L'Ente fornisce, altresì, delle caselle di posta elettronica associate a ciascuna unità organizzativa, ufficio o gruppo di lavoro il cui utilizzo è da preferire rispetto alle E-mail nominative qualora le comunicazioni siano di interesse collettivo: questo per evitare che degli utenti singoli mantengano l'esclusività su dati che possono portare alla necessità di attivazione delle procedure per l'accesso agli stessi previste nel presente regolamento.

9.3 L'iscrizione a mailing-list o newsletter esterne con l'indirizzo assegnato è concessa esclusivamente per motivi professionali o istituzionali. Prima di iscriversi occorre verificare anticipatamente l'affidabilità del sito che offre il servizio.

9.4 Assodato che le e-mail sono veicolo primario per l'infezione da virus telematici, porre particolare attenzione prima di aprire messaggi di posta in arrivo da mittenti di cui non si conosce l'identità o con contenuto sospetto o insolito, oppure che contengano allegati di tipo diverso dai formati di documento standard (es. DOC, XLS, PDF); per esempio file con estensione .exe, .com, .vbs, .scr, *.bat,

*.js e altri contengono istruzioni eseguibili e quindi potenzialmente molto pericolosi. È necessario inoltre porre molta attenzione alla credibilità del messaggio e del mittente per evitare casi di phishing o frodi informatiche. In qualunque situazione di incertezza contattare l'Amministratore di Sistema per una valutazione dei singoli casi.

9.5 Non è consentito diffondere messaggi di tipo piramidale o simili (c.d. "catena di S. Antonio") anche se il contenuto sembra meritevole di attenzione; in particolare gli appelli di solidarietà e i messaggi che informano dell'esistenza di nuovi virus. In generale è vietato l'invio di messaggi pubblicitari di prodotti di qualsiasi tipo.

9.6 Nel caso fosse necessario inviare allegati "pesanti" (superiori ai 10 MB) è opportuno ricorrere prima alla compressione dei file originali in un archivio di formato .zip o equivalenti. Nel caso di allegati ancora più voluminosi è necessario rivolgersi all'Amministratore di Sistema.

9.7 Nel caso in cui fosse necessario inviare a destinatari esterni messaggi contenenti allegati con dati personali o dati personali sensibili, è obbligatorio che questi allegati vengano preventivamente resi inintelligibili attraverso crittazione con apposito software (archiviazione e compressione con password). La password di crittazione deve essere comunicata al destinatario attraverso un canale diverso dalla mail (ad esempio per lettera o per telefono) e mai assieme ai dati criptati. Tutte le informazioni, i dati personali e/o sensibili di competenza possono essere inviati soltanto a destinatari - persone o Enti – qualificati e competenti, autorizzati al trattamento (da norme, contratti, accordi etc.).

9.8 Non è consentito l'invio automatico di messaggi di posta elettronica all'indirizzo e-mail privato (attivando per esempio un "inoltro" automatico delle e-mail entranti).

9.9 In caso di assenza prolungata è raccomandabile l'attivazione della funzione di invio automatico del messaggio "Fuori sede" facendo menzione di chi, all'interno dell'Ente, assumerà le mansioni durante l'assenza, oppure indicando un indirizzo di mail alternativo preferibilmente di tipo collettivo.

9.10 La diffusione massiva di messaggi di posta elettronica deve essere effettuata esclusivamente per motivi inerenti il servizio, possibilmente su autorizzazione del Responsabile competente. Per evitare di diffondere elenchi di indirizzi mail oltre che per impedire che le eventuali risposte siano inoltrate a tutti generando traffico eccessivo ed indesiderato, i destinatari dovranno essere messi in copia nascosta (Bcc o Ccn).

9.11 È vietato inviare messaggi di posta elettronica in nome e per conto di un altro utente, salvo sua espressa autorizzazione;

9.12 La casella di posta elettronica personale deve essere mantenuta in ordine, cancellando messaggi e documenti la cui conservazione non è più necessaria. Anche la conservazione all'interno della casella di posta di messaggi con allegati pesanti va evitata effettuando il salvataggio dell'allegato sulle condivisioni di rete e cancellando successivamente il messaggio.

9.13 I messaggi in entrata vengono sistematicamente analizzati alla ricerca di virus e malware e per l'individuazione dello spam. I messaggi che dovessero contenere virus o altri elementi potenzialmente pericolosi vengono automaticamente eliminati dal sistema.

Si informa che le comunicazioni anche elettroniche ed i documenti elettronici allegati possono avere rilevanza procedimentale e pertanto devono essere conservate per la durata prevista dalla normativa vigente.
Si informa altresì che l'Ente, per il tramite dell'Amministratore di Sistema, non controlla sistematicamente il flusso di comunicazioni mail né è dotato di sistemi per la lettura o analisi sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail.
Tuttavia, in caso di assenza improvvisa o prolungata del dipendente ovvero per imprescindibili esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio ovvero per motivi di sicurezza del sistema informatico, l'Ente per il tramite dell'Amministratore di Sistema può, secondo le

procedure indicate successivo punto 12 del presente Regolamento, accedere all'account di posta elettronica, prendendo visione dei messaggi, salvando o cancellando file.
Si informa che, in caso di cessazione del rapporto lavorativo, la mail affidata all'incaricato verrà sospesa per un periodo di 6 mesi e successivamente disattivata. Nel periodo di sospensione l'account rimarrà attivo e gestito in ricezione dall'Amministratore di Sistema o eventualmente da altro soggetto incaricato dall'Ente, che tratteranno i dati e le informazioni pervenute per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio, trasmettendone il contenuto ai responsabili del trattamento (se il messaggio ha contenuto lavorativo) ovvero cancellandolo (se il messaggio non ha contenuto lavorativo). La casella postale sarà inoltre impostata per generare una risposta automatica al mittente, invitandolo a reinviare il messaggio ad altro indirizzo mail.
Le informazioni eventualmente raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Regolamento Europeo 679/16 (GDPR).

SICUREZZA E PRIVACY DELLA POSTA ELETTRONICA

Confidenzialità

La confidenzialità della posta elettronica e della comunicazione attraverso il Web è limitata in quanto i messaggi, transitando nella rete pubblica di Internet, possono essere visionati da terzi non autorizzati. Il livello di confidenzialità di una e-mail si avvicina di più a quello di una cartolina piuttosto che a quello di una lettera. Per questa ragione è fatto divieto assoluto di comunicare informazioni classificate come riservate o dati particolari attraverso l'e-mail o attraverso il Web se non esplicitamente autorizzati dal Titolare del trattamento o da un Responsabile preposto.

Attendibilità

L'attendibilità dell'identità del mittente è molto limitata nella comunicazione via e-mail. E' relativamente facile, infatti, camuffare il mittente di una e-mail. Si richiede pertanto, ogni qual volta sia necessaria la certezza dell'identità del mittente, di verificarla con mezzi appropriati.

L'attendibilità della data ed ora esatta di invio di una e-mail è molto limitata. E' relativamente facile, infatti, modificare questi dati. Si richiede pertanto, ogni qual volta sia necessaria la certezza della data e dell'ora del messaggio, di verificarle con i mezzi appropriati.

Contenuto dei messaggi

Gli utenti devono assicurarsi che nei loro messaggi elettronici non siano inserite inconsapevolmente informazioni su User e Password utilizzate per accedere ad altre applicazioni. In particolare va usata la massima cautela nell'invio a mezzo posta elettronica di pagine internet che potrebbero contenere nell'indirizzo informazioni utili a risalire alla User/Password utilizzata.

Gli utenti sono invitati a nominare correttamente i nomi dei file allegati alle e-mail, specificando, nel caso si procedesse ad inviare documenti soggetti a modifiche e revisioni, la versione corrente del file con dei numeri progressivi.

Gli utenti sono invitati a prestare attenzione nell'utilizzo della funzione "Rispondi" e "Rispondi a tutti" nel caso il messaggio originario sia stato inviato ad un numero elevato di destinatari.

È obbligatorio controllare i file allegati di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

È vietato rispondere ad e-mail di spam in quanto una eventuale risposta conferma al mittente l'effettiva esistenza della casella e-mail provocando quindi altro spam.

Altri consigli per l'utilizzo della posta elettronica

Gli utenti sono invitati a leggere quotidianamente la posta elettronica e a rispondere in tempi ragionevoli alle e-mail ricevute. Si invitano gli utenti che hanno selezionato l'opzione di completamento automatico dell'indirizzo di prestare molta attenzione nella selezione dei destinatari.

Gli utenti devono periodicamente cancellare o organizzare in opportune cartelle la posta già letta.

Gli utenti devono sempre indicare con chiarezza (nel campo oggetto), l'argomento del proprio messaggio. E' possibile richiedere una ricevuta di corretto ricevimento della propria mail. A tale ricevuta va tuttavia assegnata una importanza relativa poiché talvolta la conferma della ricezione avviene ad opera del mail server centrale e non del destinatario ultimo del messaggio.

10 Utilizzo dei telefoni, fax, fotocopiatrici, scanner e stampanti dell'Ente

L'utente è consapevole che gli strumenti di stampa, così come anche il telefono, sono di proprietà dell'Ente e sono resi disponibili esclusivamente per rendere la prestazione lavorativa o la mansione svolta. Pertanto l'uso è concesso secondo le direttive di seguito indicate.

10.1 Il telefono affidato all'utente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa o della mansione svolta e non sono quindi consentite comunicazioni a carattere personale e/o non strettamente inerenti l'incarico stesso. La ricezione o l'effettuazione di comunicazioni a carattere personale è consentito solo nel caso di comprovata necessità ed urgenza.

10.2 Qualora venga assegnato un cellulare all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Ai cellulari e smartphone si applicano le medesime regole sopra previste per gli altri dispositivi informatici (cfr. 7 "Utilizzo di personal computer"), per quanto riguarda il mantenimento di un adeguato livello di sicurezza informatica. In particolare, se consentita, si raccomanda il rispetto delle regole per una corretta navigazione in Internet (cfr. 8).

10.3 Per gli smartphone è vietata l'installazione e l'utilizzo di applicazioni (o altresì denominate "app" nel contesto degli smartphone) diverse da quelle autorizzate dall'Amministratore di Sistema.

10.4 È vietato l'utilizzo delle fotocopiatrici per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Responsabile del Servizio di riferimento.

10.5 Per quanto concerne l'uso delle stampanti gli utenti sono tenuti a:

- 10.5.1 Stampare documenti solo se strettamente necessari per lo svolgimento delle proprie funzioni operative;
- 10.5.2 Prediligere le stampanti di rete condivise, rispetto a quelle locali/personali, per ridurre l'utilizzo di materiali di consumo (toner ed altri consumabili);
- 10.5.3 Prediligere ove possibile la stampa in bianco/nero e fronte/retro al fine di ridurre i costi.

10.6 Le stampanti e le fotocopiatrici devono essere spente in caso di inutilizzo prolungato.

10.7 Nel caso in cui si rendesse necessaria la stampa di informazioni riservate l'utente dovrà presidiare il dispositivo di stampa per evitare la possibile perdita o divulgazione di tali informazioni e persone terze non autorizzate.

L'Ente può avvalersi in relazioni agli strumenti di stampa di sistemi di reportistica d'uso e delle funzioni di log presenti negli apparati stessi ed in relazione ai telefoni fissi e mobili di tabulati del traffico telefonico opportunamente anonimizzati forniti dagli operatori telefonici o presenti nei sistemi interni. Tali registri possono essere oggetto di controllo da parte del Titolare del trattamento per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio.
I controlli possono avvenire secondo le disposizioni previste al successivo punto 12 del presente Regolamento.
Le informazioni così raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Regolamento Europeo 679/16 "General Data Protection Regulation".

11 Assistenza agli utenti e manutenzioni

11.1 L'Amministratore di Sistema può accedere ai dispositivi informatici sia direttamente, sia mediante software di accesso remoto, per i seguenti scopi:

– verifica e risoluzione di problemi sistemistici ed applicativi, su segnalazione dell'utente finale.

– verifica del corretto funzionamento dei singoli dispositivi in caso di problemi rilevati nella rete.

– necessità di aggiornamento software e manutenzione hardware e software anche preventiva.

11.2 Gli interventi tecnici posso avvenire previa informativa all'utente, quando l'intervento stesso richiede l'accesso ad aree personali dell'utente stesso. Qualora l'intervento tecnico in loco o in remoto non necessiti di accedere mediante credenziali utente, l'Amministratore di Sistema è autorizzato ad effettuare gli interventi senza il consenso dell'utente cui la risorsa è assegnata.

11.3 L'accesso in teleassistenza sui PC della rete da parte di terzi (fornitori di applicativi) deve essere per il primo accesso autorizzato dall'Amministratore di Sistema per le verifiche delle modalità di intervento. Le richieste successive, se effettuate con la medesima finalità e modalità, possono essere gestite autonomamente dall'utente finale.

11.4 Durante gli interventi in teleassistenza da parte di operatori terzi, l'utente richiedente o l'Amministratore di Sistema devono presenziare la sessione remota, in modo tale da verificare ed impedire eventuali comportamenti non conformi al presente regolamento.

12 Controlli sugli Strumenti (art. 6.1 Provv. Garante, ad integrazione dell'Informativa ex art. 13 Reg. 679/16)

12.1 Poiché in caso di violazioni contrattuali e giuridiche sia il datore di lavoro che il singolo lavoratore sono potenzialmente perseguibili con sanzioni, anche di natura penale, l'Ente verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità del proprio sistema informatico. Il datore di lavoro, infatti, può avvalersi legittimamente, nel rispetto dello Statuto dei lavoratori (art. 4, comma 2), di sistemi che consentono indirettamente il controllo a distanza (c.d. controllo preterintenzionale) e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori. Resta ferma la necessità di rispettare le procedure di informazione e di consultazione di lavoratori e sindacati in relazione all'introduzione o alla modifica di sistemi automatizzati per la raccolta e l'utilizzazione dei dati, nonché in caso di introduzione o di modificazione di procedimenti tecnici destinati a controllare i movimenti o la produttività dei lavoratori. I controlli devono essere effettuati nel rispetto dell'art. 2.2 del presente Regolamento e dei seguenti principi:

- **Proporzionalità:** il controllo e l'estensione dello stesso dovrà rivestire, in ogni caso, un carattere adeguato, pertinente e non eccessivo rispetto alla/alle finalità perseguite.
- **Trasparenza:** l'adozione del presente Regolamento ha l'obiettivo di informare gli utenti sui diritti ed i doveri di entrambe le parti.
- **Pertinenza e non eccedenza:** ovvero evitando un'interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori, così come la possibilità di controlli prolungati, costanti o indiscriminati.

12.2 L'uso degli Strumenti Informatici dell'Ente può lasciare traccia delle informazioni sul relativo uso, come analiticamente spiegato nei riquadri di cui ai punti 6 – 7 – 8 – 9 – 10 del presente Regolamento. Tali informazioni, che possono contenere dati personali eventualmente anche sensibili dell'Utente, possono essere oggetto di controlli da parte dell'Ente, per il tramite dell'Amministratore di Sistema, volti a garantire esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio, nonché per la sicurezza e la salvaguardia del sistema informatico, per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento, sostituzione, implementazione di programmi, manutenzione hardware, etc.). Gli interventi di controllo sono di due tipi, di seguito descritti al punto 12.3 e 12.4, e possono permettere all'Ente di prendere indirettamente cognizione dell'attività svolta con gli Strumenti.

12.3 **Controlli per la tutela del patrimonio, nonché per la sicurezza e la salvaguardia del sistema informatico. Controlli per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento, sostituzione, implementazione di programmi, manutenzione hardware, etc.).**

Qualora per le finalità qui sopra descritte risulti necessario l'accesso agli Strumenti e alle risorse informatiche e relative informazioni descritte ai punti 6 – 7 – 8 – 9 – 10 il Responsabile del trattamento dei dati personali per il tramite dell'Amministratore di Sistema, si atterrà al processo descritto qui di seguito (se e in quanto compatibile con lo Strumento oggetto di controllo).

i. Avviso generico a tutti i dipendenti della presenza di comportamenti anomali che possono mettere a rischio la sicurezza del sistema informativo e richiamo all'esigenza di attenersi al rispetto del presente Regolamento.

ii. Successivamente, dopo almeno 7 giorni, se il comportamento anomalo persiste, l'Ente potrà autorizzare il personale addetto al controllo, potendo così accedere alle informazioni descritte ai punti 6 – 7 – 8 – 9 – 10 con possibilità di rilevare file trattati, siti web visitati, software installati, documenti scaricati, statistiche sull'uso di risorse ecc. nel corso dell'attività lavorativa. Tale attività potrà essere effettuata in forma anonima ovvero tramite controllo del numero IP, dell'Utente e con l'identificazione del soggetto che non si attiene alle istruzioni impartite.

iii. Qualora il rischio di compromissione del sistema informativo sia imminente e grave a tal punto da non permettere l'attesa dei tempi necessari per i passaggi procedimentali descritti ai punti 1 e 2, il Responsabile del Trattamento, unitamente all'Amministratore di Sistema, potrà intervenire senza indugio sullo strumento da cui proviene la potenziale minaccia.

12.4 Controlli per esigenze produttive e di organizzazione.

Per esigenze produttive e di organizzazione si intendono – fra le altre – l'urgente ed improrogabile necessità di accedere a file o informazioni lavorative di cui si è ragionevolmente certi che siano disponibili su risorse informatiche di un Utente (quali file salvati, posta elettronica, chat, SMS, etc.) che non sia reperibile, in quanto ad esempio assente, temporaneamente irreperibile ovvero cessato.

Qualora risulti necessario l'accesso alle risorse informatiche e relative informazioni descritte ai punti 6 – 7 – 8 – 9 – 10 il Responsabile del trattamento dei dati personali, per il tramite dell'Amministratore di Sistema, si atterrà alla procedura descritta qui di seguito (se e in quanto compatibile con lo Strumento oggetto di controllo).

i. Redazione di un atto da parte del Responsabile del Servizio che comprovi le necessità produttive e di organizzazione che richiedano l'accesso allo Strumento.

ii. Incarico all'Amministratore di sistema di accedere alla risorsa con credenziali di Amministratore ovvero tramite l'azzeramento e la contestuale creazione di nuove credenziali di autenticazione dell'Utente interessato, con avviso che al primo accesso alla risorsa, lo stesso dovrà inserire nuove credenziali.

iii. Redazione di un verbale che riassuma i passaggi precedenti.

iv. In ogni caso l'accesso ai documenti presenti nella risorsa è limitato a quanto strettamente indispensabile alle finalità produttive e di organizzazione del lavoro.

v. Qualora indirettamente si riscontrino file o informazioni anche personali, esse potranno essere altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, considerato che il presente Regolamento costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal Regolamento Europeo 679/16 (GDPR).

Tutti i controlli sopra descritti avvengono nel rispetto del principio di necessità e non eccedenza rispetto alle finalità descritte nel presente Regolamento. Dell'attività sopra descritta viene redatto verbale, sottoscritto dal Responsabile del Trattamento e dall'Amministratore di Sistema che ha svolto l'attività.

In caso di nuovo accesso da parte dell'utente allo Strumento informatico oggetto di controllo, lo stesso dovrà avvenire previo rilascio di nuove credenziali (salvo diverse esigenze tecniche).

13 Conservazione dei dati

13.1 In riferimento agli articoli 5 e 6 del Reg. 679/16, ed in applicazione ai principi di diritto di accesso, legittimità, proporzionalità, sicurezza ed accuratezza e conservazione dei dati, le informazioni relative all'accesso ad Internet ed al traffico telematico (es. log di sistema e log accessi web), la cui conservazione non sia necessaria, saranno cancellati entro i termini previsti dalla normativa, salvo esigenze tecniche o di sicurezza; o per l'indispensabilità dei dati rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria o, infine, all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

13.2 L'Ente si impegna ad assumere le misure di sicurezza nel trattamento e nella conservazione di tale tipologia di dati alla luce di quanto stabilito dal Legislatore.

14 Partecipazioni a Social Media

14.1 L'utilizzo a fini promozionali di Facebook, Instagram, Twitter, Linkedin, blog, forum, social media o altri sistemi di comunicazione e di messaggistica, è gestito ed organizzato esclusivamente dall'Ente attraverso specifiche direttive ed istruzioni operative al personale a ciò espressamente addetto, rimanendo escluse iniziative individuali da parte dei singoli utenti o collaboratori.

14.2 Fermo restando il diritto della persona alla libertà di espressione, l'Ente ritiene comunque opportuno indicare agli utenti alcune regole comportamentali, al fine di tutelare tanto la propria immagine ed il patrimonio, anche immateriale, oltre che gli stessi utenti utilizzatori dei social media, fermo restando che è vietata la partecipazione agli stessi social media a titolo personale durante l'orario di lavoro.

14.3 Il presente articolo deve essere osservato dall'utente sia che utilizzi dispositivi messi a disposizione dall'Ente, sia che utilizzi propri dispositivi, sia che partecipi ai social media a titolo personale, sia che lo faccia per finalità professionali come dipendente dell'Ente e non.

14.4 La condivisione dei contenuti nei social media deve sempre rispettare e garantire la segretezza sulle informazioni considerate dall'Ente riservate ed in genere, a titolo esemplificativo e non esaustivo, sulle informazioni inerenti attività, dati contabili, finanziari, progetti, procedimenti svolti o in svolgimento presso gli uffici. 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 dell'Ente. L'utente, nelle proprie comunicazioni, non potrà quindi inserire il nominativo e il logo dell'Ente, né potrà pubblicare disegni, modelli od altro connesso ai citati diritti. Ogni deroga a quanto sopra disposto potrà peraltro avvenire solo previa specifica autorizzazione del Responsabile del Servizio di riferimento.

14.5 L'utente deve garantire la tutela della riservatezza e dignità delle persone; di conseguenza, non potrà comunicare o diffondere dati personali (quali dati anagrafici, immagini, video, suoni e voci) di colleghi e in genere di collaboratori, se non con il preventivo esplicito personale consenso di questi, e comunque non potrà postare nei social media immagini, video, suoni e voci registrati all'interno dei luoghi di lavoro, se non con il preventivo consenso del Responsabile del Servizio.

14.6 Qualora l'utente intenda usare social network, blog, forum su questioni anche indirettamente professionali (es. post su servizi, fornitori, altri enti, ecc.) egli esprimerà unicamente le proprie opinioni personali; pertanto, ove necessario od opportuno per la possibile connessione con l'Ente, l'utente dovrà precisare che le opinioni espresse sono esclusivamente personali e non riconducibili all'Ente.

15 Violazione dei dati (Data Breach)

15.1 Il Data Breach si realizza qualora all'interno dell'ente si verifichi una violazione di sicurezza che comporta - accidentalmente o in modo illecito – il trattamento illecito o non consentito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Alcuni esempi non esaustivi di situazioni di Data Breach sono:

Accesso o acquisizione di dati personali da parte di terzi non autorizzati;

Furto o perdita di dispositivi informatici contenenti dati personali (penne USB, notebook, tablet smartphone, ecc.);

Deliberata alterazione di dati personali;

Impossibilità di accedere ai dati per attacchi causati da virus, malware, ecc.;

Perdita o distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità.

15.2 Qualora si venga a conoscenza che una sospetta, presunta o effettiva violazione dei dati personali si sia verificata si è tenuti a darne immediata comunicazione al Responsabile di Servizio di riferimento, il quale provvederà nel più breve tempo possibile ad avviare la procedura di gestione del Data Breach prevista all'interno dell'Ente.

16 Sanzioni

16.1 In caso di violazione accertata delle istruzioni prescrittive di questo documento, si applica il procedimento disciplinare previsto nel contratto di lavoro e negli accordi sindacali. Qualsiasi violazione alla normativa italiana vigente da parte degli utenti sarà segnalata alle autorità competenti.

Regolamento approvato con delibera di Giunta n. 75 del 13.12.2018. In vigore dal **07.01.2019.**

Aggiornato con delibera di Giunta n. 16 del 07.04.2021.