Allegato "A" alla delibera di G.C. n° 23 in data 30.03.2021

COMUNE DI MARENO DI PIAVE

Provincia di Treviso

Regione del Veneto

REGOLAMENTO

PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI, DI INTERNET, DELLA POSTA ELETTRONICA E DEI SERVIZI DI TELEFONIA

Premessa

Il presente Regolamento intende fornire ai dipendenti e collaboratori, denominati anche autorizzati o utenti, del COMUNE DI MARENO DI PIAVE (successivamente indicato anche come Titolare) le indicazioni per una corretta e adeguata gestione delle informazioni personali, 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 i PC, notebook, smartphone, 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 dell'Ente a cui è possibile accedere tramite gli stessi, sono domicilio informatico del COMUNE DI MARENO DI PIAVE. I dati personali e le altre informazioni dell'Utente che sono registrati negli strumenti o che si possono eventualmente raccogliere tramite il loro uso, sono utilizzati per finalità istituzionali, per esigenze organizzative e produttive, per la sicurezza del lavoro ed il corretto trattamento dei dati personali, nonché per la tutela dell'immagine e del patrimonio dell'Ente.

Per tutela del patrimonio dell'Ente si intende altresì la sicurezza informatica e la tutela del sistema informatico dell'Ente. 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.

Art. 1. Oggetto e finalità

Il presente Regolamento è redatto:

1. 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";
2. in attuazione del Regolamento Europeo 679/16 sulla protezione dei dati personali (d'ora in avanti Reg. 679/16 o GDPR);
3. ai sensi delle "Linee guida del Garante per posta elettronica e internet" in Gazzetta Ufficiale n. 58 del 10 marzo 2007;
4. 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 in tutto il personale dell'Ente 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 dell'Ente e nel pieno rispetto della legge.

Si vuole tutelare i beni ed evitare condotte inconsapevoli e/o scorrette che potrebbero esporre l'Ente a problematiche di sicurezza, di immagine e patrimoniali per eventuali danni cagionati anche a terzi. L'insieme delle norme comportamentali ivi incluse, pertanto, è volto a conformare il Comune ai principi di diligenza, informazione e correttezza nell'ambito dei rapporti di lavoro, con l'ulteriore finalità di prevenire eventuali comportamenti illeciti degli utenti, pur nel rispetto dei diritti ad essi attribuiti dall'ordinamento giuridico italiano.

Art. 2. Principi generali e di riservatezza nelle comunicazioni

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 ai lavoratori. 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 dei lavoratori, 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".

Il dipendente 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 dell'Ente dei quali il dipendente / collaboratore 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 dell'Ente quando il dipendente/collaboratore 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.

d. Per le riunioni, incontri o colloqui con Utenti, cittadini, clienti, fornitori, consulenti e collaboratori dell'Ente è necessario utilizzare stanze dedicate a tale attività ovvero il proprio ufficio garantendo la riservatezza e l'applicazione dei principi di "clean desk"

Art. 3. Tutela del lavoratore

1. Alla luce dell'art. 4, comma 1, L. n. 300/1970, la regolamentazione della materia indicata nell'art. 2 del seguente 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.
2. È garantito al singolo lavoratore il controllo sui propri dati personali secondo quanto previsto dagli articoli 15-16-17-18-20-21-78 del Reg. 679/16.

Art. 4. Campo di applicazione

1. Il presente Regolamento si applica a tutto il personale del Titolare, senza distinzione di ruolo e/o di livello, nonché al personale esterno, a prescindere dal rapporto contrattuale con lo stesso intrattenuto, assegnatario di beni e risorse informatiche ovvero utilizzatore di servizi e risorse informative di pertinenza del Comune.
2. Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi anche ogni dipendente e collaboratore in possesso di specifiche credenziali di autenticazione. Tale figura potrà anche venir indicata come "autorizzato del trattamento".

Art. 5. Titolarità dei beni e delle risorse informatiche

I beni e le risorse informatiche, i servizi ICT e le reti informative costituiscono esclusiva proprietà del Comune.

Il loro utilizzo, pertanto, è consentito solo ed esclusivamente per finalità di adempimento delle mansioni lavorative o per l'espletamento di un servizio, affidati ad ogni Utente in base al rapporto in essere.

A tal fine si precisa sin d'ora che qualsivoglia dato e/o informazione trattato per mezzo dei beni e delle risorse informatiche di proprietà del Comune, sarà dallo stesso considerata come avente natura riservata.

Art. 6. Responsabilità personale dell'utente

Ogni Utente è personalmente responsabile dell'utilizzo dei beni e delle risorse informatiche affidatigli dal Comune.

A tal fine ogni Utente, nel rispetto dei principi di diligenza sottesi al rapporto instaurato con il Comune, è tenuto a tutelare (per quanto di propria competenza) il patrimonio da utilizzi impropri e non autorizzati, danni o abusi anche derivanti da negligenza, imprudenza o imperizia. L'obiettivo è quello di preservare l'integrità e la riservatezza dei beni, delle informazioni e delle risorse.

Ogni Utente è tenuto ad operare a tutela della sicurezza informatica, riportando al proprio responsabile e senza ritardo eventuali rischi di cui è a conoscenza ovvero violazioni del presente Regolamento.

Sono vietati comportamenti che possano creare un danno, anche di immagine, al Comune.

Art. 7. Amministratori del sistema

Il Comune conferisce all'amministratore di sistema, ove nominato, il compito di sovrintendere i beni e le risorse informatiche. I principali compiti, a titolo meramente esemplificativo e non esaustivo sono:

1. gestire l'hardware e il software di tutta la strumentazione informatica di appartenenza del Comune;
2. gestire la creazione, l'attivazione, la disattivazione, e tutte le relative attività amministrative degli account di rete e dei relativi privilegi di accesso alle risorse, previamente assegnati agli utenti;
3. monitorare il corretto utilizzo delle risorse di rete, dei computer e degli applicativi affidati agli utenti, purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati;
4. creare, modificare, rimuovere o utilizzare qualunque account o privilegio purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza, e della protezione dei dati;
5. rimuovere software e/o componenti hardware dalle risorse informatiche assegnate agli utenti, purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza, e della protezione dei dati;
6. provvedere alla sicurezza informatica dei sistemi informativi, nel rispetto di quanto prescritto dal GDPR;
7. utilizzare le credenziali di accesso di amministratore del sistema per accedere, anche da remoto, ai dati o alle applicazioni presenti su una risorsa informatica assegnata ad un Utente in caso di prolungata assenza, irreperibilità o impedimento dello stesso. Tale ultima attività, tuttavia, deve essere disposta per mezzo di un soggetto che rivesta quantomeno la posizione di Responsabile del Servizio e deve essere limitata altresì al tempo strettamente necessario al compimento delle attività indifferibili per cui è stato richiesto.
8. adottare adeguate politiche di sicurezza nelle configurazioni dei sistemi e degli strumenti.

Art. 8. Gestione, assegnazione e revoca delle credenziali di accesso

Le credenziali di autenticazione per l'accesso alle risorse informatiche vengono assegnate dal personale dell'Ufficio Sistemi informatici – CED, previa formale richiesta del Responsabile dell'ufficio/area 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 dell'Ufficio/area con il quale il collaboratore 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 e le relative abilitazioni necessarie allo svolgimento del lavoro. Ogni successiva variazione delle abilitazioni di accesso ai sistemi informativi dovrà essere richiesta formalmente all'Ufficio Sistemi informatici – CED dal Responsabile di riferimento.

Le credenziali di autenticazioni consistono in un codice per l'identificazione dell'utente (altresì nominati username, nome utente o user id), assegnato dall'Ufficio Sistemi informatici – CED, ed una relativa password. Ogni password è personale e riservata e dovrà essere conservata e custodita dall'autorizzato con la massima diligenza e non divulgata.

Creazione e gestione degli Account

La gestione di un account segue quanto sotto espressamente previsto:

1. l'accesso al proprio account avviene tramite l'utilizzo delle "credenziali di autenticazione" (es. "Username" e "Password"), comunicate all'Utente dal Titolare o dall'Amministratore di Sistema se nominato, che le genera, attraverso modalità che ne garantiscano la segretezza;
2. le credenziali di autenticazioni costituiscono dati da mantenere strettamente riservati e non è consentito comunicarne gli estremi a terzi;
3. se l'Utente ha il sospetto che le proprie credenziali di autenticazione siano state identificate da qualcuno, o il sospetto di un utilizzo non autorizzato del proprio account e delle risorse a questo associate, lo stesso è tenuto a modificare immediatamente la password e/o a segnalare la violazione all'amministratore del sistema nonché al Responsabile Privacy di riferimento;
4. ogni Utente è responsabile dell'utilizzo del proprio account Utente;
5. si ricorda che in caso di assenza improvvisa o prolungata del lavoratore, per improrogabili necessità legate all'attività lavorativa o per la sicurezza ed operatività delle risorse informatiche del Comune, si riserva la facoltà di accedere a qualsiasi dotazione e/o apparato assegnato in uso all'Utente per mezzo dell'intervento dell'Amministratore di Sistema o del Responsabile della Privacy (Titolare).

Gestione e utilizzo delle password

Dopo la prima comunicazione delle credenziali di autenticazione, l'Utente ha il compito di modificare prontamente, al suo primo utilizzo, la propria password, procedendo allo stesso modo almeno ogni 90 giorni.

L'Utente deve utilizzare password di adeguata robustezza, che deve rispettare le seguenti regole:

1. utilizzare almeno 8 caratteri alfanumerici, inclusi i caratteri speciali (#, %, etc.);
2. utilizzare almeno tre delle seguenti categorie: un carattere maiuscolo, un carattere minuscolo, un numero, un carattere non alfanumerico tipo "@#§£$%...";
3. non deve includere parti del nome, cognome e/o comunque elementi a lui agevolmente riconducibili;
4. evitare l'utilizzo di password comuni e/o prevedibili;
5. proteggere con la massima cura la riservatezza della password ed utilizzarla entro i limiti di autorizzazione concessi.

Il codice per l'identificazione (user-id o username) deve essere univoco ed assegnato ad un solo soggetto; esso non può essere assegnato ad altri autorizzati, neppure in tempi diversi.

Si ricorda che scrivere la password su post-it o altri supporti (ivi compresa la sua memorizzazione sul telefono/smartphone) non è conforme alla normativa e costituisce violazione del presente Regolamento.

Cessazione degli Account

Le credenziali di autenticazione (user-id e password) devono essere disattivate nei seguenti casi:

1. Nel caso di cessazione del rapporto di lavoro con il dipendente/collaboratore. Il Responsabile dell'Ufficio/area di riferimento dovrà comunicare formalmente e preventivamente all'Ufficio Sistemi informatici – CED la data effettiva a partire dalla quale le credenziali saranno disabilitate.
2. Immediatamente, nel caso in cui il dipendente/collaboratore perda la qualità che gli consentiva di accedere allo strumento: ciò non accade solo se la persona cessa di lavorare, ma può ad esempio avvenire anche se l'autorizzato viene trasferito da un ufficio all'altro, con conseguente cambio delle mansioni e degli ambiti di trattamento dei dati personali, che rendesse necessaria l'attribuzione di una nuova chiave.
3. In ogni caso, entro tre mesi di mancato utilizzo. Fa ovviamente eccezione il caso delle credenziali che sono state preventivamente autorizzate per soli scopi di gestione tecnica, il cui utilizzo assume generalmente caratteristiche di sporadicità.

Qualora vi sia richiesta di reset password di un utente a qualsiasi titolo, perché, per esempio, sussiste il dubbio che terzi ne siano venuti a conoscenza o perché dimenticata, l'AdS o il Titolare procederà a riassegnare una nuova password temporanea al fine di consentire all'utente l'accesso ai sistemi presso cui è accreditato, con l'impegno di modificarla subito dopo nei termini sopra individuati.

Art. 9. Utilizzo degli Strumenti elettronici (PC, notebook, smartphone e altri strumenti con relativi software e applicativi)

1. Il dipendente/collaboratore è consapevole che gli Strumenti forniti sono e rimangono di proprietà del Comune di Mareno di Piave e devono essere utilizzati esclusivamente per lo svolgimento delle proprie mansioni lavorative e comunque per finalità strettamente attinenti l'attività svolta. Ognuno è responsabile dell'utilizzo delle dotazioni informatiche ricevute in assegnazione. Ogni utilizzo non inerente all'attività lavorativa è vietato in quanto può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Ciascun dipendente/collaboratore si deve quindi attenere alle seguenti regole di utilizzo degli strumenti.
2. L'accesso agli Strumenti dell'Ente è protetto da password; per l'accesso devono essere utilizzati Username e password assegnate dall'Ufficio Sistemi informatici – CED. A tal proposito si rammenta che essi sono strettamente personali e l'utente è tenuto a conservarli nella massima segretezza.
3. Il Personal Computer, notebook, smartphone, tablet ed ogni altro hardware deve essere custodito con cura da parte degli assegnatari evitando ogni possibile forma di danneggiamento e segnalando tempestivamente al personale dell'Ufficio Sistemi informatici – CED ogni malfunzionamento e/o danneggiamento. Non è consentita l'attivazione della password d'accensione (BIOS), senza preventiva autorizzazione da parte dell'Ufficio Sistemi informatici – CED.
4. Non è consentito all'utente modificare le caratteristiche hardware, software e configurazioni impostate sugli strumenti assegnati, salvo preventiva autorizzazione da parte del personale dall'Ufficio Sistemi informatici – CED.
5. Il PC e gli altri dispositivi devono essere utilizzati con hardware e software autorizzati dal Comune. Per utilizzare software o applicativi non presenti nella dotazione standard fornita, si necessita di espressa autorizzazione del Responsabile del servizio a seguito di una valutazione da parte dell'AdS.
6. È fatto divieto di cedere in uso, anche temporaneo, le attrezzature e i beni informatici a soggetti terzi.
7. Il Titolare si riserva la facoltà di rimuovere qualsiasi elemento hardware la cui installazione non sia stata appositamente e preventivamente prevista o autorizzata.
8. L'utente è tenuto a scollegarsi dal sistema, o bloccare l'accesso (con un programma salvaschermo (screensaver) protetto da password o effettuare il log-out dalla sessione) 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 e con la sessione attiva può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.
9. Agli utenti autorizzati del trattamento dei dati è fatto divieto l'accesso contemporaneo con lo stesso account da più postazioni PC.
10. Le informazioni archiviate sul PC locale devono essere esclusivamente quelle necessarie all'attività lavorativa assegnata.
11. Costituisce buona regola la pulizia periodica degli archivi memorizzati sul proprio PC, con cancellazione dei file obsoleti o non più utili.
12. La gestione dei dati su PC è demandata all'utente utilizzatore che dovrà provvedere a memorizzare sulle condivisioni dell'Ente dati che possono essere utilizzati anche da altri utenti, evitando di mantenere l'esclusività su di essi.
13. Non è consentito installare autonomamente programmi informatici, software ed ogni altro applicativo non autorizzato espressamente dal Titolare;
14. Gli operatori dell'Ufficio Sistemi informatici – CED possono in qualunque momento procedere alla rimozione di ogni file o applicazione che riterranno essere pericolosi per la sicurezza dei PC, della rete locale e dei server dell'Ente, nonché tutte le impostazioni eventualmente configurate che possano interferire con il corretto funzionamento dei servizi informatici dell'Ente.
15. È obbligatorio consentire l'installazione degli aggiornamenti di sistema o del software antivirus che vengono proposti automaticamente, al primo momento disponibile, in modo tale da mantenere il PC sempre protetto.
16. È onere dell'utente sospendere ogni attività in caso di minacce virus o altri malfunzionamenti, segnalando prontamente l'accaduto all'amministratore del sistema;
17. È vietato utilizzare il PC per l'acquisizione, la duplicazione e/o la trasmissione illegale di opere protette da copyright.
18. È vietato l'utilizzo di supporti di memoria (chiavi USB, CD, DVD o altri supporti) per il salvataggio di dati trattati tramite gli strumenti dell'Ente, salvo che il supporto utilizzato sia stato fornito dall'Ufficio Sistemi informatici – CED. In tale caso, il supporto fornito può essere utilizzato esclusivamente per finalità lavorative.
19. È inibita ed è vietata l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.
20. È disattivata l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file. Nel caso in cui venga eseguito un file che contiene istruzioni automatizzate (macro), all'utente viene chiesta e data comunque la possibilità di attivare il programma. È responsabilità dell'utente garantire sull'origine del file stesso.
21. È assolutamente vietato connettere al PC qualsiasi periferica non autorizzata preventivamente dall'Ufficio Sistemi informatici – CED.
22. È assolutamente vietato connettere alla rete locale qualsiasi dispositivo (PC esterni, router, switch, modem, etc.) non autorizzato preventivamente dall'Ufficio Sistemi informatici – CED.

23. Nel caso in cui l'utente dovesse notare comportamenti anomali del PC, l'utente stesso è tenuto a comunicarlo tempestivamente all'Ufficio Sistemi informatici – CED.
24. I PC portatili utilizzati all'esterno (riunioni, incontri, convegni, ecc..) o in luoghi di facile accesso (sala consiglio, sala giunta, ecc..), in caso di allontanamento, devono essere custoditi in un luogo protetto.
25. Le postazioni PC devono essere spente al termine dell'attività svolta o in caso di inutilizzo prolungato.
26. l'Utente deve segnalare con la massima tempestività all'amministratore del sistema ovvero al proprio Responsabile di riferimento eventuali guasti tecnici, problematiche tecniche o il cattivo funzionamento delle apparecchiature.

Per quanto concerne la gestione dei computer portatili, oltre a quanto sopra indicato, l'Utente ha l'obbligo di custodirli con diligenza e in luogo protetto durante gli spostamenti, rimuovendo gli eventuali file elaborati prima della sua riconsegna. Non è consentito all'Utente caricare o inserire all'interno del portatile qualsiasi dato personale non attinente con l'attività lavorativa svolta. In ogni caso, al fine di evitare e/o ridurre al minimo la possibile circolazione di dati personali sull'apparecchio, si ricorda agli utenti di cancellare tutti i dati eventualmente presenti prima di consegnare il portatile agli uffici competenti per la restituzione o la riparazione.

Nel caso in cui l'Utente vi conservi, contrariamente alle direttive impartitegli, dati di natura personale, il Comune in nessun caso potrà essere ritenuto responsabile della salvaguardia o della perdita di tali dati. L'AdS ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento viene effettuato esclusivamente su chiamata dell'Utente e in sua presenza e previo consenso del lavoratore.

I log relativi all'utilizzo di Strumenti, reperibili nella memoria degli Strumenti stessi ovvero sui Server o sui router dell'Ente, nonché i file con essi trattati sono registrati e possono essere oggetto di controllo da parte del Titolare del trattamento, attraverso l'Ufficio Sistemi informatici – CED dell'Ente, 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 art. 19 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".

Art. 10. Utilizzo di strumenti personali del dipendente/collaboratore per l'espletamento dell'attività lavorativa in modalità agile (smartwork)

Gli strumenti di proprietà personale dell'Utente quali computer PC; notebook portatili e telefoni cellulari/smartphone possono essere utilizzati per l'espletamento dell'attività lavorativa in modalità agile nel rispetto delle disposizioni riportate nel presente Regolamento, per le parti comunque applicabili, nonché di queste ulteriori disposizioni:

1. È obbligo utilizzare sistemi operativi per i quali è attualmente garantito il supporto e l'aggiornamento;
2. Effettuare costantemente gli aggiornamenti di sicurezza del tuo sistema operativo;
3. Assicurarsi che i software di protezione del proprio sistema operativo (Firewall, Antivirus, ecc.) siano abilitati e costantemente aggiornati;
4. Assicurarsi che gli accessi al sistema operativo siano protetti da una password sicura e comunque conforme alle regole riportare in questo Regolamento;
5. Utilizzare l'accesso alla rete internet attraverso connessioni sicure (es. Wi-Fi adeguatamente protette);
6. Bloccare l'accesso al sistema e configurare il blocco automatico quando la postazione rimane incustodita;
7. Effettuare sempre il log-out dai servizi/portali utilizzati dopo che si è conclusa l'attività lavorativa;
8. Creare un profilo dedicato allo smartworking con diritti minimali ed utilizzarlo in via esclusiva per il lavoro;
9. Non conservare alcun dato personale relativo all'attività lavorativa nel dispositivo (PC, notebook, smartphone, pen-drive o storage personali) nemmeno temporaneamente;
10. Utilizza preferibilmente le risorse in cloud messe a disposizione dal Titolare;
11. Utilizzare esclusivamente software necessari per svolgere il tuo lavoro;
12. Non memorizzare credenziali di accesso all'utilizzo delle risorse dell'ente sulle postazioni personali;
13. Non lasciare incustodito il dispositivo di lavoro;
14. Adottare ogni cautela a protezione del dispositivo utilizzato, specialmente in caso di spostamenti;
15. Comunicare senza ritardo ogni tipo di incidente da cui potrebbe derivare una violazione di dati personali

Art. 11. Utilizzo di software

Premesso che l'installazione di software privi di regolare licenza non è consentita in nessun caso, gli utenti dovranno ottenere espressa autorizzazione del Responsabile Privacy/Amministratore di Sistema per installare o comunque utilizzare qualsiasi programma o software dotato di licenza non proprietaria ("freeware" o "shareware").

Il Titolare richiama l'attenzione degli utenti su alcuni aspetti fondamentali che l'Utente è tenuto ad osservare per un corretto utilizzo del software:

1. il Titolare acquista le licenze d'uso dei software da vari fornitori esterni. L'Utente, pertanto, è soggetto a limitazioni nell'utilizzo di tali programmi e della relativa documentazione e non ha il diritto di riprodurlo in deroga ai diritti concessigli. Tutti gli utenti sono quindi tenuti a utilizzare il software entro i limiti specificati nei contratti di licenza;

2. non è consentito fare né il download né l'upload tramite internet di software non autorizzato;
3. il Titolare, sulla scorta di quanto disposto dalle normative a tutela della proprietà intellettuale e del diritto d'autore, ricorda che le persone coinvolte nella riproduzione illegale del software sono responsabili sia civilmente che penalmente e quindi possono essere condannate al pagamento dei danni e anche alla reclusione;
4. in nessun caso il Titolare utilizza software o altri strumenti di tipo Key Log per la registrazione delle operazioni eseguite da tastiera;
5. il Titolare non tollererà la duplicazione illegale del software.

Art. 12. Dispositivi di memoria portatili

Per dispositivi di memoria portatili si intendono tutti quei dispositivi che consentono di copiare o archiviare dati, file o documenti esternamente al computer. Sono considerati tali CD-ROM, DVD, penne o chiavi di memoria USB, fotocamere digitali, dischi rigidi esterni, etc.

L'utilizzo di tali supporti risponde alle direttive che di seguito si riportano:

1. non è consentito utilizzare supporti rimovibili personali per lo scambio dati, se non preventivamente autorizzati per iscritto dal Titolare;
2. è onere dell'Utente custodire i supporti magnetici contenenti dati sensibili e giudiziari in armadi chiusi a chiave, onde evitare che il loro contenuto possa essere trafugato e/o alterato e/o distrutto.

Si precisa che, ove autorizzati in base a quanto sopra disposto, una volta connessi all'infrastruttura informatica del Titolare, i dispositivi saranno soggetti (ove compatibili) al presente Regolamento.

Art. 13. Utilizzo della rete del Comune di Mareno di Piave

1. Per l'accesso alle risorse informatiche del Comune, attraverso la rete locale, ciascun utente deve essere in possesso di credenziali di autenticazione secondo l'art. 8.
2. È proibito accedere alla rete e nei sistemi informativi utilizzando credenziali di altre persone.
3. L'accesso alla rete garantisce all'utente la disponibilità di condivisioni di rete (cartelle su server) nelle quali vanno inseriti e salvati i files di lavoro, organizzati per area/ufficio o per diversi criteri o per obiettivi specifici di lavoro. Tutte le cartelle di rete possono ospitare esclusivamente contenuti professionali. Pertanto è vietato il salvataggio sui server dell'Ente, ovvero sugli Strumenti, di documenti non inerenti l'attività lavorativa, quali a titolo esemplificativo documenti, fotografie, video, musica, pratiche personali, sms, mail personali, film e quant'altro. Ogni materiale personale rilevato dall'Ufficio Sistemi informatici – CED 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 art. 13 del presente Regolamento, ferma ogni ulteriore responsabilità civile, penale e disciplinare. Tutte le risorse di memorizzazione, diverse da quelle citate all'art. 9, non sono sottoposte al controllo regolare degli Amministratori di Sistema e non sono oggetto di backup periodici. A titolo di esempio e non esaustivo si citano: il disco primario (C:) o altri dischi locali dei singoli PC, la cartella "Documenti" o "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 dell'Ente, 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.
4. Senza il consenso del Titolare, è vietato trasferire documenti elettronici dai sistemi informativi e Strumenti dell'Ente a device esterni (hard disk, chiavette, CD, DVD e altri supporti).
5. Senza il consenso dell'Ufficio Sistemi informatici – CED è vietato salvare documenti elettronici dell'Ente (ad esempio pervenuti via mail o salvati sul Server o sullo Strumento in dotazione) su repository esterne (quali ad esempio Dropbox, GoogleDrive, OneDrive, ecc.) o altri servizi esterni.
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.
7. Il Comune di Mareno di Piave mette a disposizione al personale dell'Ufficio Sistemi informatici – CED la possibilità di accedere alle risorse informatiche dell'Ente anche dall'esterno dei confini dell'Ente, mediante rete VPN (Virtual Private Network), un canale privato e criptato verso la rete interna.
8. All'interno della sede municipale è resa disponibile ai membri della Giunta anche una rete senza fili, c.d. "Wi-Fi Mareno". Tale rete consente l'accesso esclusivamente ad internet. L'accesso mediante rete Wi-Fi viene anche concesso a consulenti, professionisti, tecnici e fornitori che nell'ambito di un rapporto contrattuale con Comune di Mareno di Piave devono accedere ad internet. L'impostazione della connessione Wi-Fi sarà effettuata da personale dell'Ufficio Sistemi informatici – CED.
9. L'Ufficio Servizio informatici – CED 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 dell'Ente.

I log relativi all'uso del File System e della intranet dell'Ente, 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'Ufficio Sistemi informatici – CED dell'Ente, 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 art. 19 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”.

Art. 14. 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.

Ogni Utente potrà essere abilitato, dal Titolare, alla navigazione Internet. Con il presente Regolamento si richiama gli utenti ad una particolare attenzione nell’utilizzo di Internet e dei servizi relativi, in quanto ogni operazione posta in essere è associata all’”Indirizzo Internet Pubblico” assegnato al Titolare stesso.

Internet è uno strumento messo a disposizione degli utenti per uso professionale. Ciascun lavoratore, pertanto, deve quindi usare la rete Internet in maniera appropriata, tenendo presente che ogni sito web può essere governato da leggi diverse da quelle vigenti in Italia; l'Utente deve quindi prendere ogni precauzione a tale riguardo.

Ciascun dipendente/collaboratore si deve attenere alle seguenti regole di utilizzo della rete Internet e dei relativi servizi.

1. È ammessa solo la navigazione in siti considerati correlati con la prestazione lavorativa. L’accesso è consentito tramite apparato firewall dell’Ente con le sue policy di sicurezza debitamente implementate e aggiornate, ad es. i siti istituzionali, i siti degli Enti locali, di fornitori e partner dell’Ente. Per facilitare il rispetto delle predette regole, il Comune si riserva, per mezzo dell’Ufficio Sistemi informatici – CED, la facoltà di configurare specifici filtri che inibiscono l’accesso ai contenuti ivi non consentiti e che prevengono operazioni non correlate all’attività lavorativa (es. upload, restrizione nella navigazione, download di file o software).
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.
3. È vietato a chiunque il download di qualunque tipo di software gratuito (freeware) o shareware prelevato da siti Internet, se non espressamente autorizzato dall’Ufficio Sistemi informatici – CED.
4. L’Ente si riserva di bloccare l’accesso a siti “a rischio” attraverso l’utilizzo di blacklist pubbliche in continuo aggiornamento e di predisporre filtri, basati su sistemi euristici di valutazione del livello di sicurezza dei siti web remoti, tali da prevenire operazioni potenzialmente pericolose o comportamenti impropri. In caso di blocco accidentale di siti di interesse dell’Ente, contattare l’Ufficio Sistemi informatici – CED per uno sblocco selettivo.
5. Nel caso in cui, per ragioni di servizio, si necessiti di una navigazione libera dai filtri del suddetto firewall, è necessario richiedere lo sblocco mediante una mail indirizzata all’Ufficio Sistemi informatici – CED, ed in copia al Responsabile dell’Area competente, 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 gli artt. 14.1, 14.2 e 14.3 del presente Regolamento. Al termine dell’attività gli addetti dell’Ufficio Sistemi informatici – CED ripristineranno i filtri nella situazione iniziale.
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 gestiti dal servizio finanziario, con il rispetto delle normali procedure di acquisto.
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’Ufficio Sistemi informatici – CED e del Responsabile del Servizio/Area previo parere tecnico degli stessi Amministratori.
8. È assolutamente vietata la partecipazione a Forum non professionali, ai 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).
9. È assolutamente vietata la navigazione in siti e la memorizzazione di documenti informatici di natura oltraggiosa, pornografica, pedopornografica e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
10. È assolutamente vietato lo scambio e/o la condivisione (es. i c.d. sistemi di Peer-to-Peer) a qualsiasi titolo, anche se non a scopo di lucro, di materiale audiovisivo, cinematografico, fotografico, informatico, etc., protetto da copyright;
11. È consentito l’uso di strumenti di messaggistica istantanea, per permettere un’efficace e comoda comunicazione tra i colleghi, mediante i soli strumenti autorizzati dall’Ufficio Sistemi informatici – CED. 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.
12. 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’Ufficio Sistemi informatici – CED, 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 dell’Ente, l’Ente registra per non più di 365 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 può trattare i dati di navigazione riferendoli specificatamente ad un singolo nome utente. In tali casi i controlli avverranno nelle forme indicate al successivo art. 19 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".

Art. 15. 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. La Posta Elettronica di tutti gli account con suffisso "@comune.marenodipiave.tv.it" rappresenta, ormai, una forma di comunicazione analoga a quella scritta su carta intestata del Comune.

Si ricorda che attraverso l'e-mail, gli utenti rappresentano pubblicamente l'Ente e per questo motivo viene richiesto di utilizzare tale sistema in modo lecito, professionale e comunque tale da riflettere l'immagine.

Ad ogni Utente titolare di un account, il Titolare provvede ad assegnare una casella di posta elettronica individuale e quindi ciascun dipendente/collaboratore si deve attenere alle seguenti regole di utilizzo dell'indirizzo di Posta elettronica.

1. Ad ogni utente viene fornito un account e-mail dell'Ente nominativo, generalmente coerente con il modello nome.cognome@comune.marenodipiave.tv.it. L'utilizzo dell'e-mail deve essere limitato esclusivamente a scopi dell'Ente, ed è assolutamente vietato ogni utilizzo di tipo privato. L'utente a cui è assegnata una casella di posta elettronica è responsabile del corretto utilizzo della stessa.
2. I servizi di posta elettronica devono essere utilizzati in coerenza con lo scopo della struttura: si ricorda a tutti gli utenti che l'account e-mail è uno strumento di proprietà del Titolare ed è conferito in uso per l'esclusivo svolgimento delle mansioni affidate.
3. 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 dell'Ente. Tali caselle devono essere utilizzate per la ricezione dei messaggi, mentre per le risposte o gli invii, è consigliabile utilizzare la casella di posta individuale assegnata.
4. Per i criteri di gestione ed utilizzo delle password di accesso all'e-mail si fa riferimento a quanto indicato nel precedente art. 8 per quanto applicabili;
5. L'iscrizione a mailing-list o newsletter esterne con il proprio indirizzo dell'Ente personale è concessa esclusivamente per motivi professionali. Prima di iscriversi occorre verificare anticipatamente l'affidabilità del sito che offre il servizio.
6. Allo scopo di garantire sicurezza alla rete dell'Ente, evitare 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 *.exe, *.com, *.vbs, *.htm, *.scr, *.bat, *.js, *.pif. ecc… È necessario porre molta attenzione, inoltre, alla credibilità del messaggio e del mittente per evitare casi di phishing o frodi informatiche. In qualunque situazione di incertezza contattare l'Ufficio Sistemi informatici – CED per una valutazione dei singoli casi.
7. Non è consentito diffondere messaggi del tipo "catena di S. Antonio" o di tipologia simile 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.
8. Nel caso fosse necessario inviare allegati "pesanti" (superiori a 15 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'Ufficio Sistemi informatici – CED .
9. Nel caso in cui fosse necessario inviare a destinatari esterni messaggi contenenti allegati con dati personali o dati personali particolari, è obbligatorio che questi allegati vengano preventivamente resi inintelligibili attraverso criptazione con apposito software (archiviazione e compressione con password). La password di criptazione 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 dell'Ente, i dati personali e/o sensibili di competenza dell'Ente possono essere inviati soltanto a destinatari - persone o Enti – qualificati e competenti.
10. Non è consentito l'invio automatico di e-mail all'indirizzo e-mail privato (attivando per esempio un "inoltro" automatico delle e-mail entranti), anche durante i periodi di assenza (es. ferie, malattia, infortunio ecc.). In questa ultima ipotesi, è raccomandabile utilizzare un messaggio "Fuori Ufficio" facendo menzione di chi, all'interno dell'Ente, assumerà le mansioni durante l'assenza, oppure indicando un indirizzo di mail alternativo. Rivolgersi all'Ufficio Sistemi informatici – CED per tale eventualità.
11. In caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, qualora non fosse possibile attivare la funzione di risposta automatica o l'inoltro automatico su altre caselle dell'Ente e si debba conoscere il contenuto dei messaggi di posta elettronica, il titolare della casella di posta ha la facoltà di delegare un altro dipendente (fiduciario) per verificare il contenuto di messaggi e per inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Sarà compito del Responsabile dell'Area competente assicurarsi che sia redatto un verbale attestante quanto avvenuto e che sia informato il lavoratore interessato alla prima occasione utile;

12. La diffusione massiva di messaggi di posta elettronica deve essere effettuata esclusivamente per motivi inerenti il servizio, possibilmente su autorizzazione del Responsabile dell'Area competente. Per evitare che le eventuali risposte siano inoltrate a tutti, generando traffico eccessivo ed indesiderato, i destinatari dovranno essere messi in copia nascosta (Bcc o Ccn) se la tipologia del messaggio lo consente.
13. È vietato inviare posta elettronica in nome e per conto di un altro utente, salvo sua espressa autorizzazione;
14. È vietato trasmettere e-mail di tipo professionale al proprio indirizzo privato.
15. 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 di messaggi con allegati pesanti è da evitare per quanto possibile, preferendo, in alternativa, il salvataggio dell'allegato sulle condivisioni dell'Ente.
16. I messaggi in entrata vengono sistematicamente analizzati alla ricerca di virus e malware e per l'eliminazione dello spam. I messaggi che dovessero contenere virus vengono eliminati dal sistema e il mittente/destinatario viene avvisato mediante messaggio specifico.
17. Ogni utente è responsabile in via esclusiva del contenuto di messaggi, file di testo, immagini, file audio e qualsiasi allegato da egli pubblicato o trasmesso attraverso i sistemi di Posta Elettronica e lo stesso ha l'obbligo di controllare gli allegati di posta elettronica ricevuti prima del loro utilizzo.
18. Gli allegati provenienti da mittenti sconosciuti non devono essere aperti in quanto possono essere utilizzati come veicolo per introdurre programmi dannosi (es. virus).
19. È vietato utilizzare la casella di posta elettronica per inviare, ricevere o scaricare allegati contenenti video, brani musicali, etc., salvo che questo non sia funzionale all'attività prestata in favore dell'Ente (es: presentazioni o materiali video).
20. Il software di gestione della posta elettronica deve essere impostato in modo che sia disattivata l'apertura automatica dei messaggi di posta elettronica, inibendo così l'anteprima del messaggio.
21. Ogni utente può collegarsi a siti internet contenuti all'interno di messaggi (link) solo quando vi sia comprovata sicurezza sul contenuto degli stessi.
22. Alla fine del messaggio di posta da inviare, deve essere apposto un messaggio di "disclaimer" (Es. - *"Le informazioni contenute in questo messaggio e-mail, ed i suoi eventuali allegati, sono da considerarsi "dati confidenziali" ad uso esclusivo del destinatario. Ove il lettore di questo messaggio non sia il destinatario, o la persona autorizzata a trattarlo o consegnarlo, questi è informato che qualsiasi modifica, divulgazione, distribuzione o copia è assolutamente proibita. In caso di ricezione per errore di questo messaggio e-mail informate il mittente immediatamente a mezzo e-mail e poi distruggete il documento ed i suoi eventuali allegati. Eventuali divulgazioni, usi ed abusi tanto del messaggio che degli eventuali allegati saranno immediatamente perseguiti ai sensi della normativa vigente ed in ogni sede prevista."*)
23. Rispetto all'utilizzo della posta elettronica certificata (PEC) si applicano, ove compatibili, le presenti disposizioni.

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'Ufficio Sistemi informatici – CED, non controlla sistematicamente il flusso di comunicazioni e-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 qualora il lavoratore non possa attivare il messaggio automatico di assenza/"Fuori ufficio" (anche avvalendosi di servizi webmail) ovvero per imprescindibili esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente ovvero per motivi di sicurezza del sistema informatico, l'Ente per il tramite dell'Ufficio Sistemi informatici – CED può, secondo le procedure indicate successivo art. 19.4 del presente Regolamento, accedere all'account di posta elettronica dell'utente, prendendo visione dei messaggi, salvando o cancellando file.

In questo caso, si procederà come segue:

1. sarà preventivamente richiesto all'utente di farlo lui stesso, se possibile, tramite web mail;
2. la verifica del contenuto dei messaggi sarà effettuata per il tramite dal Segretario e/o Responsabile di Servizio;
3. al termine della verifica verrà comunicato all'utente l'attività svolta dall'AdS dal Segretario e/o Responsabile di Servizio.

Si informa che, in caso di cessazione del rapporto lavorativo, la mail dell'Ente affidata all'autorizzato verrà sospesa per un periodo di 6 mesi e successivamente disattivata. Nel periodo di sospensione l'account rimarrà attivo e visibile ad un soggetto incaricato dall'Ente solo in ricezione, che tratterà i dati e le informazioni pervenute per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente, trasmettendone il contenuto ad altri dipendenti (se il messaggio ha contenuto lavorativo) ovvero cancellandolo (se il messaggio non ha contenuto lavorativo). Il sistema in ogni caso genererà una risposta automatica al mittente, invitandolo a reinviare il messaggio ad altro indirizzo mail dell'Ente. 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 "General Data Protection".

In ogni caso, il Titolare si riserva il diritto di conservare i messaggi di posta elettronica che riterrà rilevanti.

Art. 16. Utilizzo dei fax, fotocopiatrici, scanner e stampanti dell'Ente

Il dipendente è consapevole che gli strumenti di stampa, così come anche il telefono dell'Ente, sono di proprietà del Comune di Mareno di Piave e sono resi disponibili all'utente per rendere la prestazione lavorativa. Pertanto ne viene concesso l'uso esclusivamente per tale fine.

1. È vietato l'utilizzo delle fotocopiatrici dell'Ente per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Responsabile di Ufficio.
2. Per quanto concerne l'uso delle stampanti gli utenti sono tenuti a:
    1. Stampare documenti solo se strettamente necessari per lo svolgimento delle proprie funzioni operative e di ritirarli prontamente dai vassoi delle stampanti comuni;
    2. Prediligere le stampanti di rete condivise, rispetto a quelle locali/personali, per ridurre l'utilizzo di materiali di consumo (toner ed altri consumabili);
    3. Prediligere la stampa in bianco/nero e fronte/retro al fine di ridurre i costi, se possibile.
3. Le stampanti e le fotocopiatrici dell'Ente devono essere spente ogni sera prima di lasciare gli uffici o in caso di inutilizzo prolungato.
4. 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.
5. L'utilizzo dei fax per l'invio di documenti che hanno natura strettamente confidenziale, è generalmente da evitare. Nei casi in cui questo sia necessario, si deve preventivamente avvisare il destinatario, in modo da ridurre il rischio che persone non autorizzate possano venirne a conoscenza, e successivamente chiedere la conferma telefonica di avvenuta ricezione.

Art. 17. Utilizzo di strumenti di fonia mobile e/o di connettività in mobilità

Il Titolare mette a disposizione, a seconda del ruolo o della funzione del singolo Utente, impianti di telefonia fissa e mobile, nonché dispositivi - quali smartphone e tablet - che consentono di usufruire della navigazione in internet tramite rete dati e/o del servizio di telefonica tramite rete cellulare.

L'Utente dovrà attenersi ai limiti di traffico previsti dal Titolare, potendo in caso contrario la stessa richiedere il rimborso dei costi sostenuti per il superamento degli stessi.

Non sono consentite comunicazioni a carattere personale e/o non strettamente inerenti l'attività lavorativa stessa. La ricezione o l'effettuazione di comunicazioni a carattere personale è consentito solo nel caso di comprovata necessità ed urgenza.

A tal fine si informano gli utilizzatori dei servizi di fonia, che il Titolare potrà richiedere ai provider di telefonia i dettagli necessari ad effettuare controlli sull'utilizzo ed i relativi costi di traffico effettuato nel tempo al fine di una corretta fatturazione.

I controlli saranno eseguiti secondo le modalità descritte all'art. 19 del presente Regolamento.

Il Titolare si riserva la facoltà, qualora dall'esame del traffico di una singola utenza rilevi uno scostamento significativo rispetto alla media del consumo, di richiedere un tabulato analitico delle chiamate effettuate dalla SIM in incarico all'Utente per il periodo interessato.

Ai dispositivi mobili dell'Ente si applicano le medesime regole sopra previste per gli altri dispositivi informatici (crf. art. 9 "Utilizzo degli Strumenti elettronici"), per quanto riguarda il mantenimento di un adeguato livello di sicurezza informatica, per le parti applicabili. In particolare si raccomanda il rispetto delle regole per una corretta navigazione in Internet (cfr. art.14 "Utilizzo di internet").

L'utilizzo dei dispositivi ivi disciplinati risponde alle regole che di seguito si riportano:

1. ogni Utente assegnatario del dispositivo è responsabile dell'uso appropriato dello stesso, e, conseguentemente, anche della sua diligente conservazione.
2. I dispositivi devono essere dotati di password di sicurezza (cd. codice pin del dispositivo) che ne impedisca l'utilizzo da parte di soggetti non autorizzati. A tal fine si precisa che:
    1. il CODICE PIN di sblocco dovrà essere composto di n. 4/6 cifre numeriche;
    2. il CODICE PIN dovrà essere modificato dall'assegnatario con cadenza al massimo semestrale;
3. ogni Utente deve adottare le necessarie e dovute cautele per assicurare la segretezza della password e, qualora ritenga che un soggetto non autorizzato possa esserne venuto a conoscenza, dovrà provvedere immediatamente a cambiarla dandone comunque comunicazione al Titolare;
4. in caso di danneggiamento l'Utente assegnatario dovrà darne immediato avviso al Titolare, in caso di furto o smarrimento del dispositivo mobile in oggetto, l'Utente assegnatario dovrà denunciare il fatto alle competenti autorità pubbliche e darne successivo avviso al Titolare; ove detti eventi siano riconducibili ad un comportamento negligente, imprudente dell'Utente e/o comunque a sua colpa nella custodia del bene, lo stesso sarà ritenuto unico responsabile dei danni derivanti;
5. in caso di furto o smarrimento il Titolare si riserva la facoltà di attuare la procedura di remote-wipe (cancellazione da remoto di tutti i dati sul dispositivo), rendendo il dispositivo inutilizzabile e i dati in esso contenuti irrecuperabili;

6. non è consentito all'Utente caricare o inserire all'interno del dispositivo o SIM qualsiasi dato personale non attinente con l'attività lavorativa svolta. In ogni caso, al fine di evitare e/o ridurre al minimo la possibile circolazione di dati personali sull'apparecchio, si ricorda agli assegnatari di cancellare tutti i dati eventualmente presenti prima di consegnare il cellulare agli uffici competenti per la restituzione o la riparazione;
7. è consentito all'Utente effettuare riprese, fotografie, registrazioni di suoni con qualsiasi tipologia di apparecchiatura elettronica esclusivamente adatta a scopi lavorativi/professionali;
8. non è consentito all'Utente effettuare procedure di jailbreak, modifiche del firmware o procedure di sblocco a vario titolo, tali da permettere l'illegittima installazione di software e/o applicazioni coperte da copyright;
9. è onere dell'Utente mantenere installato software antivirus sullo smartphone; in caso di problemi l'Utente potrà rivolgersi all'AdS;
10. l'eventuale installazione di applicazioni, sia gratuite che a pagamento, sugli smartphone e tablet deve essere espressamente autorizzata, rimanendo, diversamente, a carico dell'Utente le spese che il Titolare dovrà sostenere, nonché le responsabilità derivanti dall'installazione non autorizzata;
11. salvo diversi specifici accordi, al momento della consegna del tablet o smartphone l'Utente è tenuto a verificare la disattivazione del sistema di geolocalizzazione potenzialmente attivabile sugli smartphone e tablet, consapevole che, in caso contrario, il Titolare potrebbe venire a conoscenza, seppur incidentalmente, dei dati relativi alla posizione del dispositivo stesso e del suo assegnatario.

Art. 18. Assistenza agli utenti e manutenzioni

1. L'Ufficio Sistemi informatici – CED può accedere ai dispositivi informatici dell'Ente sia direttamente, sia mediante software di accesso remoto, per i seguenti scopi:
    1. verifica e risoluzione di problemi sistemistici ed applicativi, su segnalazione dell'utente finale.
    2. verifica del corretto funzionamento dei singoli dispositivi in caso di problemi rilevati nella rete.
    3. richieste di aggiornamento software e manutenzione preventiva hardware e software.
2. Gli interventi tecnici posso avvenire previo consenso dell'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, il personale dell'Ufficio Sistemi informatici – CED è autorizzato ad effettuare gli interventi senza il consenso dell'utente cui la risorsa è assegnata.
3. L'accesso in teleassistenza sui PC della rete dell'Ente richiesto da terzi (fornitori e/o altri) deve essere autorizzato dall'Ufficio Sistemi informatici – CED, per le verifiche delle modalità di intervento per il primo accesso. Le richieste successive, se effettuate con la medesima modalità, possono essere gestite autonomamente dall'utente finale.
4. Durante gli interventi in teleassistenza da parte di operatori terzi, l'utente richiedente od il personale dell'Ufficio Sistemi informatici – CED devono presenziare la sessione remota, in modo tale da verificare ed impedire eventuali comportamenti non conformi al presente Regolamento.

Art. 19. Controlli sugli Strumenti (art. 6.1 Provv. Garante, ad integrazione dell'Informativa ex art. 13 Reg. 679/16)

Fermo restando il diritto del Titolare di effettuare controlli sull'effettivo adempimento della prestazione lavorativa nonché sul corretto utilizzo dei beni e servizi informatici (artt. 2086, 2087 e 2104 c.c.), i controlli posti in essere, saranno sempre tali da evitare ingiustificate interferenze con i diritti e le libertà fondamentali dei lavoratori e non saranno costanti, prolungati e indiscriminati, nel rispetto del principio di pertinenza e non eccedenza.

Il Titolare, in linea con quanto prescritto dall'ordinamento giuridico italiano (art. 4, Statuto dei Lavoratori), esclude la configurabilità di forme di controllo aventi direttamente ad oggetto l'attività lavorativa dell'Utente.

Ciò nonostante non si esclude che, per ragioni organizzative e produttive, di tutela del patrimonio ovvero per esigenze dettate dalla sicurezza, si utilizzino sistemi informatici, impianti, apparecchiature o dispositivi dai quali derivi la possibilità di controllo a distanza dell'attività dei lavoratori. In tal caso tali strumenti verranno valutati e subordinati rispetto alla normativa di settore, ed i dati acquisiti con lo strumento verranno trattati secondo l'informativa privacy data.

1. Poiché in caso di violazioni contrattuali e giuridiche, sia l'Ente, sia 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. 3.2 del presente Regolamento e dei seguenti principi:
    I. **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, ma resterà sempre entro i limiti minimi.
    II. **Trasparenza**: l'adozione del presente Regolamento ha l'obiettivo di informare gli utenti sui diritti ed i doveri di entrambe le parti.
    III. **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.

2. L'uso degli Strumenti Informatici dell'Ente può lasciare traccia delle informazioni sul relativo uso, come analiticamente spiegato nei riquadri di cui agli artt. 7, 8, 9, 10 del presente Regolamento. Tali informazioni, che possono contenere dati personali eventualmente anche particolari dell'Utente, possono essere oggetto di controlli da parte dell'Ente, per il tramite dell'Ufficio Sistemi informatici – CED, volti a garantire esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente, 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 agli artt. 19.3 e 19.4) e possono permettere all'Ente di prendere indirettamente cognizione dell'attività svolta con gli strumenti.
3. Controlli per la tutela del patrimonio dell'Ente, 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, ecc.).

Qualora per le finalità qui sopra descritte risulti necessario l'accesso agli Strumenti e alle risorse informatiche e relative informazioni descritte agli artt. 7, 8, 9, 10 il Responsabile del trattamento dei dati personali per il tramite dell'Ufficio Sistemi informatici – CED, 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 agli artt. 7, 8, 9, 10 con possibilità di rilevare files 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 dell'Ente sia imminente e grave a tal punto da non permettere l'attesa dei tempi necessari per i passaggi procedimentali descritti ai punti i e ii, il Responsabile del Trattamento, unitamente all'amministratore di sistema, può intervenire senza indugio sullo strumento da cui proviene la potenziale minaccia.

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 files 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, ecc.) 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 agli artt. 7, 8, 9, 10 il Responsabile del trattamento dei dati personali, per il tramite dell'Ufficio Sistemi informatici – CED, 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 dell'Area competente che comprovi le necessità produttive e di organizzazione che richiedano l'accesso allo Strumento.
II. Incarico all'Ufficio Sistemi informatici – CED 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 "General Data Protection".

5. **I controlli non autorizzati**

In ogni caso il Titolare non può in alcun caso utilizzare sistemi da cui derivino forme di controllo a distanza dell'attività lavorativa che permettano di ricostruire l'attività del lavoratore.

Per tali s'intendono, a titolo meramente esemplificativo e non esaustivo:

I. la lettura e la registrazione sistematica dei messaggi di posta elettronica, al di là di quanto necessario per fornire e gestire il servizio di posta elettronica stesso;
II. la riproduzione e la memorizzazione sistematica delle pagine internet visualizzate da ciascun Utente, dei contenuti ivi presenti, e del tempo di permanenza sulle stesse;
III. la lettura e la registrazione dei caratteri inseriti dal lavoratore tramite tastiera o dispositivi analoghi;
IV. l'analisi occulta di computer portatili affidati in uso.

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 dal personale dell'Ufficio Sistemi informatici – CED 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).

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 “General Data Protection”.

Art. 20. Conservazione dei dati

1. In riferimento agli articoli 5 e 6 del Reg. 679/16 e in applicazione ai principi di diritto di accesso, legittimità, proporzionalità, sicurezza ed accuratezza e conservazione dei dati, le informazioni relative all’accesso ad Internet e dal traffico telematico (log di sistema e log di firewall), la cui conservazione non sia necessaria, saranno cancellati entro i termini indicati nel presente Regolamento, 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.
2. La 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.

Art. 21 Partecipazioni a Social Media

1. L’utilizzo a fini promozionali di Facebook, Twitter, YouTube, Linkedin, dei blog e dei forum, anche professionali (ed altri siti o social media) 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.
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 dell’Ente, anche immateriale, quanto i propri collaboratori, i propri clienti e fornitori, gli altri partners, oltre che gli stessi utenti utilizzatori dei social media, fermo restando che è vietata la partecipazione agli stessi social media durante l’orario di lavoro/espletamento della prestazione lavorativa.
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.
4. La condivisione dei contenuti nei social media deve sempre rispettare e garantire la segretezza sulle informazioni dell’Ente, nel rispetto del segreto d’ufficio, segreto professionale e privacy.

Art. 22. Sanzioni disciplinari

1. È fatto obbligo a tutti i dipendenti/collaboratori/utenti di osservare le disposizioni portate a conoscenza con il presente Regolamento.
2. L’eventuale violazione di quanto previsto dal presente Regolamento – rilevante anche ai sensi degli art. 2104 e 2105 c.c. - potrà comportare l’applicazione di sanzioni disciplinari in base a quanto previsto dall’art. 3 del Codice di comportamento dei dipendenti e dall’art. 7 dello Statuto dei Lavoratori.
3. Il Comune avrà cura di informare senza ritardo (e senza necessità di preventive contestazioni e/o addebiti formali) le autorità competenti, nel caso venga commesso un reato, o la cui commissione sia ritenuta probabile o solo sospettata, tramite l’utilizzo illecito o non conforme dei beni e degli strumenti informatici.
4. Si precisa, infine, che in caso di violazione accertata da parte degli utenti delle regole e degli obblighi esposti in questo Regolamento, il Responsabile Privacy/AdS si riserva la facoltà di sospendere, bloccare o limitare gli accessi di un account, quando appare ragionevolmente necessario per proteggere l’integrità, la sicurezza e/o la funzionalità dei propri beni e strumenti informatici.

Art. 23 Comunicazioni

1. Il presente Regolamento è messo a disposizione degli utenti, per la consultazione, al momento dell’assegnazione di un account Utente e sempre reperibile nel Portale Privacy della intranet e nella cartella dei Regolamenti comunali.