COMUNE DI PIOVENE ROCCHETTE

PROVINCIA DI VICENZA

REGOLAMENTO SULL'UTILIZZO DEGLI STRUMENTI INFORMATICI E SULLA POSTA ELETTRONICA ISTITUZIONALE

Approvato con deliberazione di C.C. n. __ del 30.09.2019

1. PREMESSE....4
1.1 Scopo del Regolamento....4
1.2 Fonti normative....4
1.3 Principi generali....4
2. REGOLE DI COMPORTAMENTO GENERALI....4
....4
2.2 Obbligo di riservatezza....5
2.3 Impostazioni....5
3. REGOLE DI COMPORTAMENTO SPECIALI RELATIVE ALL'UTILIZZO DEI PERSONAL COMPUTER E ALTRI STRUMENTI....5
3.1 Credenziali di autenticazione....5
3.2 Installazione e utilizzo di programmi....5
3.3 Supporti esterni....5
3.4 Violazioni di sicurezza....5
3.5 Spegnimento del PC e allontanamento dalla propria posizione....6
3.6 Salvataggio dei documenti....6
3.7 Assenze....6
3.8 Antivirus....6
3.9 Utilizzo di notebook, tablet e altri strumenti....7
3.10 Informazioni sulla conservazione dei dati....7
4. REGOLE DI COMPORTAMENTO SPECIALI RELATIVE ALL'USO DELLA RETE DEL COMUNE...7
4.1 Accesso alla rete informatica....7
4.2 Cartelle di rete....7
4.3 Informazioni sulla conservazione dei dati....8
5. CREDENZIALI DI AUTENTICAZIONE....8
5.1. Assegnazione delle credenziali di autenticazione....8
5.2 Composizione delle credenziali di autenticazioni e della password....8
5.3 Divieti e regole di comportamento....8
5.4 Conoscenza della password da parte di terzi....9
5.5 Sospensione....9
5.6 Cessazione....9
6. UTILIZZO DI INTERNET....9
6.1 Finalità lavorative nell'uso di internet....9
6.2 Partecipazioni a social network....10
6.3 Regole di comportamento....10
6.4 Informazioni sulla conservazione dei dati....10
7. UTILIZZO DELLA POSTA ELETTRONICA....11

7.1 Finalità lavorative nell'utilizzo della posta elettronica....11
7.2 Regole di comportamento....11
7.3 Assenza dell'Utente....12
7.4 Spam ed antispam....12
7.5 Disattivazione della casella di posta elettronica....12
7.6 Informazioni sulla conservazione dei dati....12
8. UTILIZZO DI APPARATI DI TELEFONIA, FAX, FOTOCOPIATRICI, SCANNER E STAMPANTI....13
8.1 Finalità lavorative nell'utilizzo degli apparati di telefonia e di stampa....13
8.2 Password....13
8.3 Informazioni sulla conservazione dei dati....14
9. OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY E DELLA L. 300/1970....14
10. ASSISTENZA AGLI UTENTI E MANUTENZIONI....14
11. CONTROLLI....15
11.1 Principi generali....15
11.2 Controlli per la tutela del patrimonio del Comune, per la sicurezza e la salvaguardia del sistema informatico. Controlli per ulteriori motivi tecnici e/o manutentivi....15
11.3 Controlli per esigenze produttive e di organizzazione....15
12. CONSERVAZIONE DEI DATI....16
13. SANZIONI....16
14. ENTRATA IN VIGORE....16

1. PREMESSE

1.1 Scopo del Regolamento

Il presente regolamento (di seguito il "Regolamento") si prefigge di determinare le regole per il corretto ed adeguato accesso ed utilizzo di tutti gli apparati (di seguito gli "Apparati") e dei sistemi informatici e telematici, sia hardware che software (di seguito i "Sistemi"), del Comune di Piovene Rocchette (di seguito "il Comune" o il "Titolare del trattamento"), da parte:

- dei dipendenti del Comune, senza distinzione di ruolo e/o livello;

- di tutti i collaboratori, stagisti, consulenti esterni;

di seguito gli "Utenti".

I dati personali e le altre informazioni dell'Utente, che sono registrati negli Apparati e nei Sistemi e che si possono eventualmente raccogliere tramite il loro uso, sono utilizzati per finalità istituzionali, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio del Comune, compresa la sicurezza informatica e la tutela del sistema informatico del Comune. Tali informazioni sono utilizzabili per 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, nel rispetto di quanto previsto dal Regolamento UE 679/16 (Regolamento generale sulla protezione dei dati).

1.2 Fonti normative

Il presente Regolamento è stato redatto sulla base del Regolamento UE 679/16 ("Regolamento generale sulla protezione dei dati" o "GDPR"), del d.lgs. n. 196/2003 ("Codice privacy"), della L. n. 300/1973 ("Statuto dei Lavoratori") e delle "Linee Guida del Garante per posta elettronica e internet" pubblicate nella Gazzetta Ufficiale n. 58 del 10.03.2007, nonché degli altri provvedimenti in materia pronunciati dal Garante per la protezione dei dati personali (di seguito "il Garante").

1.3 Principi generali

Il presente Regolamento si fonda sui medesimi principi espressi nel GDPR, in particolare:

a) principio di necessità, secondo il quale i sistemi ed i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione dei dati personali e dei dati identificativi in relazione alle finalità perseguite (articoli 5 e 6 GDPR);

b) principio di correttezza, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori, in modo da renderli adeguatamente consapevoli;

c) principio di pertinenza e non eccedenza, secondo cui i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime, nella misura meno invasiva possibile.

2. REGOLE DI COMPORTAMENTO GENERALI

2.1 Finalità lavorative nell'utilizzo degli Apparati e dei Sistemi

L'utilizzo degli Apparati e dei Sistemi è consentito solo agli Utenti per finalità connesse allo svolgimento delle prestazioni lavorative in favore del Comune, nel rispetto e nei limiti del presente Regolamento. Gli Utenti sono tenuti ad utilizzare gli Apparati e i Sistemi con diligenza, correttezza e buona fede, astenendosi dal porre in essere comportamenti che configurino illeciti di qualunque genere o violazione di diritti di persone fisiche o giuridiche. Gli Utenti devono custodire con cura i PC, notebook, tablet e ogni altro

dispositivo di proprietà del Comune, evitando ogni possibile forma di danneggiamento e segnalando tempestivamente ogni malfunzionamento e/o danneggiamento. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

Non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

2.2 Obbligo di riservatezza

Gli Utenti sono tenuti a non rivelare a terzi le caratteristiche degli Apparati e dei Sistemi, le modalità di funzionamento e le norme di sicurezza adottate.

2.3 Impostazioni

E' vietato, salvo autorizzazione dell'Amministratore di Sistema, modificare le impostazioni degli Apparati e dei Sistemi.

3. REGOLE DI COMPORTAMENTO SPECIALI RELATIVE ALL'UTILIZZO DEI PERSONAL COMPUTER E ALTRI STRUMENTI

3.1 Credenziali di autenticazione

L'accesso al personal computer (di seguito "PC") è protetto da credenziali di autenticazione, costituite da un codice identificativo associato a una parola chiave (di seguito "password").

3.2 Installazione e utilizzo di programmi

Non è consentito all'Utente di modificare le caratteristiche impostate sul proprio PC, salvo autorizzazione esplicita dell'Amministratore di Sistema.

Non è consentito installare autonomamente programmi provenienti dall'esterno salvo previa autorizzazione dell'Amministratore di Sistema, perché sussiste il grave pericolo di portare virus informatici e di alterare la stabilità delle applicazioni del PC.

Non è consentito l'uso di programmi diversi da quelli in uso presso il Comune.

E' obbligatorio consentire l'installazione degli aggiornamenti di sistema che vengono proposti automaticamente, al primo momento disponibile, in modo da mantenere il PC sempre protetto.

3.3 Supporti esterni

L'installazione ed utilizzo di eventuali supporti esterni (chiavette USB, modem, masterizzatori e simili) avviene sotto l'esclusiva responsabilità dell'Utente. Ogni Utente deve pertanto prestare la massima attenzione a tali supporti, avvertendo immediatamente l'Amministratore di Sistema nel caso in cui siano rilevati virus e adottando quanto previsto al successivo punto 3.8 del presente Regolamento in relazione alle procedure di protezione antivirus.

3.4 Violazioni di sicurezza

Nel caso in cui l'Utente venga a conoscenza di una qualsiasi violazione di sicurezza che possa comportare la violazione di dati personali, dovrà contattare immediatamente il Sindaco, il Responsabile della protezione dei dati (di seguito "DPO") e l'Amministratore di Sistema, in modo da permettere il tempestivo avvio delle procedure da seguire in caso di "data breach" (articoli 33 e seguenti GDPR).

3.5 Spegnimento del PC e allontanamento dalla propria posizione

Il PC deve essere spento o disconnesso dall'utente che ne ha effettuato l'accesso al termine di ogni giornata lavorativa, al momento di lasciare gli uffici a fine giornata o prima, in caso di uscita anticipata dal luogo di lavoro.

Durante la giornata lavorativa, nelle pause, o, comunque, nei momenti in cui il PC rimanga anche solo temporaneamente incustodito per allontanamento dalla postazione di lavoro, deve essere attivato il blocco temporaneo della sessione di lavoro con l'apposita sequenza illustrata dall'Amministratore di Sistema. 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.

3.6 Salvataggio dei documenti

I dipendenti dovranno provvedere a memorizzare sulle condivisioni del Comune i documenti e i dati che possono essere utilizzati anche da altri Utenti, evitando di mantenere l'esclusività su di essi. Le informazioni archiviate sul PC locale devono essere esclusivamente quelle necessarie all'attività lavorativa assegnata.

Gli Utenti sono tenuti ad effettuare delle pulizie periodiche degli archivi memorizzati sul proprio PC, con cancellazione dei file obsoleti o non più utili.

3.7 Assenze

In caso di assenza dell'Utente, al fine di garantire la sicurezza e la continuità delle attività istituzionali, e qualora sussistano necessità d'ufficio, il capoufficio, potrà richiedere all'Amministratore di Sistema di accedere alle informazioni necessarie per il proseguimento dell'attività. L'intervento sarà comunicato all'Utente e verrà redatto un apposito verbale nel quale riportare le necessità che abbiano determinato l'intervento. Dopo l'accesso, l'Utente dovrà provvedere al cambio password.

3.8 Antivirus

Ogni Utente deve tenere comportamenti tali da ridurre il rischio di attacchi al sistema informatico aziendale mediante malware, deve astenersi dall'aprire allegati ai messaggi di posta elettronica quando provengano da indirizzo o mittenti sconosciuti, nonché astenersi dal navigare su siti internet che appaiono non sicuri. I messaggi di posta elettronica di cui non si è certi della provenienza non devono mai essere aperti, in quanto tali messaggi possono far parte di attività di "pishing" (messaggi che simulano, nella grafica e nel contenuto, quello di una istituzione nota al destinatario ma provengono in realtà da soggetti il cui scopo è il furto di identità). Tali messaggi devono immediatamente essere segnalati all'Amministratore di Sistema.

L'attività di installazione, attivazione e manutenzione dei firewall, dei programmi antimalware e di sicurezza della navigazione è riservata all'Amministratore di Sistema. E' vietato quindi disattivare e/o disinstallare e/o modificare nella loro impostazione iniziale i firewall, i programmi antimalware e di sicurezza della navigazione installata sia a livello di server che di ogni singolo client, in quanto pericoloso per il proprio computer e per l'intera rete del Comune. É cura di ogni singolo Utente verificare l'avvenuto aggiornamento del sistema antivirus presente nel proprio PC.

Nel caso il software antivirus rilevi la presenza di un virus, l'Utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer nonché segnalare prontamente l'accaduto all'Amministratore di Sistema.

Ogni dispositivo magnetico di provenienza esterna al Comune dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato all'Amministratore di Sistema.

3.9 Utilizzo di notebook, tablet e altri strumenti

Le disposizioni previste dai punti 3.1 a 3.8 si applicano anche ai notebook, tablet e altri strumenti con relativi software e applicativi. In caso di smarrimento e/o furto, l'Utente assegnatario ha l'obbligo di informare per iscritto, entro 24 ore, anche via e-mail, il Sindaco, il DPO e l'Amministratore di Sistema, e ciò anche al fine di attivare le procedure relative al "data breach". L'Utente dovrà anche sporgere denuncia presso le sedi competenti, inoltrando poi copia della denuncia al Comune.

3.10 Informazioni sulla conservazione dei dati

I log relativi all'utilizzo dei PC, reperibili nella memoria dei PC stessi ovvero sui server, 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 del Comune. I controlli possono avvenire secondo le disposizioni previste dall'articolo 11 del presente Regolamento.

Le informazioni eventualmente raccolte sono altresì utilizzabili per tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, considerato che il presente Regolamento costituisce adeguata informazione sulle modalità d'uso degli strumenti e sulla effettuazione dei controlli ai sensi del GDPR.

4. REGOLE DI COMPORTAMENTO SPECIALI RELATIVE ALL'USO DELLA RETE DEL COMUNE

4.1 Accesso alla rete informatica

Per l'accesso alla rete informatica ciascun Utente deve essere in possesso delle specifiche credenziali di autenticazione. Le password d'ingresso alla rete e ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite. E' assolutamente proibito entrare nella rete e nei programmi con altri nomi Utente.

4.2 Cartelle di rete

Le cartelle di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità (a titolo esemplificativo, documenti, fotografie, video, musica, pratiche personali, e-mail, film e quant'altro). Su queste unità vengono svolte regolari attività di controllo, amministrazione e back up da parte dell'Amministratore di Sistema. Tutte le informazioni devono essere salvate sempre e soltanto nelle cartelle di rete presenti nei server del Comune.

Tutte le unità diverse da quelle comuni non sono oggetto di back up. Di conseguenza, le stesse non devono ospitare dati di interesse del Comune, poiché non sono garantite la sicurezza e la protezione contro la eventuale perdita dei dati. Pertanto, la responsabilità dei salvataggi dei dati ivi contenuti è a carico del singolo Utente.

L'Amministratore di Sistema, a seguito di interventi di sicurezza informatica e/o di manutenzione/aggiornamento, può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza sia sui PC degli Utenti sia sulle unità di rete, ferma restando ogni responsabilità civile, penale e disciplinare. Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. E' da evitare un'archiviazione ridondante.

E’ vietato salvare documenti elettronici del Comune su Dropbox, GoogleDrive, OneDrive e similari, salvo autorizzazione del Responsabile dell’Ufficio, del gruppo GDPR nominato dal Comune e dell’Amministratore di Sistema.

4.3 Informazioni sulla conservazione dei dati

I log relativi all’uso della rete del Comune, nonché i file salvati o trattati su server sono registrati e possono essere oggetto di controllo da parte del Titolare, attraverso l’Amministratore di Sistema, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio del Comune. I controlli possono avvenire secondo le disposizioni previste dall’articolo 11 del presente Regolamento.

Le informazioni eventualmente raccolte sono altresì utilizzabili per tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, considerato che il presente Regolamento costituisce adeguata informazione sulle modalità d’uso degli strumenti e sulla effettuazione dei controlli ai sensi del GDPR.

5. CREDENZIALI DI AUTENTICAZIONE

5.1. Assegnazione delle credenziali di autenticazione

Le credenziali di autenticazione, costituite da un codice identificativo associato ad una password, vengono assegnate dall’Amministratore di Sistema, previa richiesta del Responsabile dell’Ufficio. Il codice identificativo non può essere assegnato ad altri Utenti, neanche in tempi diversi. Le credenziali di autenticazione sono disattivate: a) in caso di mancato utilizzo per almeno sei mesi; b) in caso di perdita della qualità di dipendente e/o di collaboratore e/o di agente da parte dell’Utente.

5.2 Composizione delle credenziali di autenticazioni e della password

Le credenziali di autenticazione sono costituite da un codice identificativo (user id) e da una password, che deve essere custodita dall’Utente con la massima diligenza e non divulgata.

La password deve essere composta da almeno 8 (otto) caratteri e non contenere riferimenti agevolmente riconducibili all’Utente (username, nomi o date relative alla persona o a un suo familiare). La password deve essere modificata dall’Utente al primo utilizzo e successivamente, almeno ogni sei mesi, che si riducono a tre mesi nel caso in cui il dipendente tratti dati particolari come definiti dall’art. 9 del GDPR.

5.3 Divieti e regole di comportamento

E’ vietato usare le credenziali di autenticazione di altro Utente nonché consentire ad altro Utente o a terzi di utilizzare le proprie credenziali di autenticazione.

La password deve essere immediatamente modificata dall’Utente qualora sospetti che la stessa non sia più segreta. Nel caso in cui l’Utente sospetti che la password sia stata utilizzata da persone non autorizzate, dovrà essere immediatamente informato l’Amministratore di Sistema.

5.4 Conoscenza della password da parte di terzi

Qualora un Utente o qualsiasi altro soggetto dovesse venire a conoscenza della password di un altro Utente, è tenuto a darne immediata notizia all’interessato, astenendosi dal qualsiasi utilizzo o divulgazione della stessa. L’interessato dovrà provvedere alla immediata modifica della stessa.

5.5 Sospensione

L’Amministratore di Sistema, per l’espletamento delle proprie funzioni nonché in caso di emergenza o di assenza dell’Utente, ha la facoltà in qualunque momento di sospendere e/o modificare l’operatività dei profili

personali degli Utenti (compresa la posta elettronica e la navigazione internet), nonché di accedere a qualunque apparato, sistema o informazione.

5.6 Cessazione

In caso di cessazione del rapporto di lavoro con il dipendente/collaboratore, il Responsabile dell'Ufficio deve comunicare formalmente e preventivamente all'Amministratore di Sistema la data effettiva a partire dalla quale saranno disattivate le credenziali.

6. UTILIZZO DI INTERNET

6.1 Finalità lavorative nell'uso di internet

Internet può essere utilizzato solo per finalità collegate all'attività lavorativa svolta dall'Utente. In via meramente esemplificativa e non esaustiva, l'Utente non può utilizzare internet per:

– scaricare software senza l'autorizzazione dell'Amministratore di Sistema (fermo restando la necessità di verificare le condizioni di licenza d'uso dei programmi, che sono protetti dalla legge sul diritto di autore), inclusi i software "peer to peer" per lo scambio e diffusione tramite internet di materiale protetto dalla legge sul diritto di autore;

– navigare su siti pornografici o pedopornografici (quest'ultima fattispecie penalmente rilevante per l'Utente);

– navigare su siti di *"gaming on line"* di qualsiasi genere e natura;

– navigare su siti di social network di qualsiasi natura (in via esemplificativa e non esaustiva: Facebook, Twitter, Instagram, ecc...), utilizzare chat line (ad esclusione delle chat autorizzate per esigenze lavorative), iscriversi a forum non professionali.

– effettuare ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dal Responsabile d'ufficio e comunque nel rispetto delle normali procedure di acquisto;

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

Il Comune si riserva di bloccare l'accesso a siti considerati "a rischio" attraverso l'utilizzo di blacklist pubbliche in continuo aggiornamento e di predisporre dei filtri, basati su sistemi euristici di valutazione del livello di sicurezza dei siti web remoti, tali da prevenire operazioni potenzialmente pericolose o comportamenti impropri. Nel caso in cui, per ragioni di servizio, si necessiti di una navigazione libera dai filtri del suddetto proxy, è necessario richiedere lo sblocco mediante una mail indirizzata all'Amministratore di Sistema, ed in copia al Responsabile di Ufficio, 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 11 del presente Regolamento. Al termine dell'attività l'Amministratore di Sistema ripristinerà i filtri nella situazione iniziale.

6.2 Partecipazioni a social network

L'utilizzo a fini promozionali dei social network – quali Facebook, dei blog e dei forum, anche professionali – verrà gestito ed organizzato esclusivamente dal Comune attraverso specifiche direttive ed istruzioni operative al personale a ciò espressamente addetto, rimanendo escluse iniziative individuali da parte dei singoli Utenti (conformemente a quanto disposto al precedente punto 6.1).

Fermo restando il pieno ed inderogabile diritto della persona alla libertà di espressione ed al libero scambio di idee ed opinioni, il Comune ritiene comunque opportuno indicare agli Utenti alcune regole comportamentali, al fine di tutelare tanto la propria immagine e il patrimonio, 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 viene vietata la partecipazione agli stessi social network durante l'orario di lavoro (salvo il personale autorizzato all'uso della pagina Facebook del Comune). La policy qui dettata deve venir seguita dagli Utenti sia che utilizzino dispositivi messi a disposizione dal Comune, sia che utilizzino propri dispositivi, sia che partecipino ai social network a titolo personale, sia che lo facciano per finalità professionali, come dipendenti dello stesso Comune.

La condivisione dei contenuti nei social network deve sempre rispettare e garantire la segretezza sulle informazioni del Comune, nel rispetto del segreto d'ufficio, del segreto professionale e della privacy. L'Utente deve garantire la tutela della privacy delle persone; di conseguenza, non potrà comunicare o diffondere dati personali (quali dati anagrafici, immagini, video, suoni e voci) di colleghi e in genere di collaboratori del Comune, se non con il preventivo personale consenso di questi.

L'Utente risponde personalmente dei propri comportamenti e deve astenersi dal porre in essere, nei confronti in genere di terzi e specificatamente verso il Comune, i colleghi, i clienti ed i fornitori, attività che possano essere penalmente o civilmente rilevanti; a titolo esemplificativo, sono quindi vietati comportamenti ingiuriosi, diffamatori e denigratori, discriminatori o che configurano molestie.

6.3 Regole di comportamento

Gli Utenti sono tenuti a:

– modificare le impostazioni del browser utilizzato per la navigazione in internet;

– non eseguire download di file eseguibili o documentati da siti web dei quali non siano certi della provenienza e dell'assenza di rischi per il PC.

6.4 Informazioni sulla conservazione dei dati

Il Comune non effettua la memorizzazione sistematica delle pagine web visualizzate dal singolo Utente, né controlla con sistemi automatici i dati di navigazione dello stesso.

Al fine di garantire la sicurezza dei sistemi informatici, nonché per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio del Comune, il Comune registra per un periodo limitato i dati di navigazione (file di log riferiti al traffico web), con modalità inizialmente volte a precludere l'immediata e diretta identificazione degli Utenti, mediante opportune aggregazioni. Solo in casi eccezionali e di comprovata urgenza rispetto alle finalità sopra descritte, il Comune può trattare i dati di navigazione riferendoli specificatamente ad un singolo Utente. In tali casi, in controlli verranno eseguite nelle forme indicate al punto 11 del presente Regolamento.

Le informazioni eventualmente raccolte sono altresì utilizzabili per tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, considerato che il presente Regolamento costituisce adeguata informazione sulle modalità d'uso degli strumenti e sulla effettuazione dei controlli ai sensi del GDPR.

7. UTILIZZO DELLA POSTA ELETTRONICA

7.1 Finalità lavorative nell'utilizzo della posta elettronica

La posta elettronica messa a disposizione dal Comune è uno strumento di lavoro e può essere utilizzata solo per finalità connesse all'attività lavorativa dell'Utente. Ogni utilizzo diverso è vietato.

Ad ogni Utente viene messo a disposizione un account e-mail del Comune, generalmente così predisposto: m.r@comune.piovene-rocchette.vi.it (iniziale del nome punto cognome). L'Utente è responsabile del corretto utilizzo della casella di posta elettronica.

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

– l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es. mp3) non legati all'attività lavorativa;

– l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list;

– la partecipazione a catene telematiche (o c.d. "di Sant'Antonio"). Se si dovessero peraltro ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al personale dell'Amministratore di Sistema.

Non è consentito l'invio automatico di e-mail all'indirizzo e-mail privato (attivando, ad esempio, un inoltro automatico delle e-mail entranti), anche durante i periodi di assenza (es. ferie, malattia, ecc.). In quest'ultima ipotesi, è opportuno seguire le istruzioni di cui al punto 7.3 del presente Regolamento.

7.2 Regole di comportamento

Gli Utenti sono tenuti a rispettare le seguenti regole di condotta:

– è vietato inviare posta elettronica in nome e per conto di un altro Utente, salvo sua espressa autorizzazione;

– la casella di posta elettronica deve essere mantenuta in ordine, cancellando documenti inutili;

– è obbligatorio porre la massima attenzione nell'aprire i file allegati ai messaggi di posta elettronica;

– gli Utenti devono provvedere all'archiviazione nelle preposte cartelle di rete di tutti i documenti rilevanti ai fini istituzionali allegati alle e-mail in modo da garantire le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità.

7.3 Assenza dell'Utente

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

In caso di assenza non programmata (ad es. per malattia) la procedura - qualora non possa essere attivata dal lavoratore avvalendosi del servizio webmail entro due giorni - verrà attivata a cura dell'Amministratore di Sistema, su richiesta del capo ufficio.

Sarà comunque consentito al capo ufficio o a persona individuata nel Comune, sentito l'Utente, accedere alla casella di posta elettronica dell'Utente per ogni ipotesi in cui si renda necessario (ad es.: mancata attivazione della funzionalità di cui sopra, assenza non programmata ed impossibilità di attendere i due giorni di cui al punto che precede), in conformità dei punti 7.6 e 11.3 del presente Regolamento. In questo caso, verrà redatto un atto nel quale riportare le ragioni di necessità che hanno determinato l'accesso alla posta elettronica. Dopo l'accesso, l'Utente dovrà provvedere al cambio password.

7.4 Spam ed antispam

L'Utente che dovesse ricevere messaggi indesiderati può comunicarlo all'Amministratore di Sistema. E' vietato aprire messaggi di cui si ignori la provenienza o dare seguito alle istruzioni ivi contenute.

7.5 Disattivazione della casella di posta elettronica

La casella di posta elettronica, unitamente alle credenziali di autenticazione per l'accesso alla rete, viene immediatamente disattivata al momento della conclusione del rapporto di lavoro che ne giustificava l'assegnazione. Il Comune adotta dei sistemi automatici volti ad informarne i terzi e a fornire indirizzi alternativi riferiti all'attività istituzionale.

7.6 Informazioni sulla conservazione dei dati

Le comunicazioni, anche elettroniche, ed i documenti elettronici allegati possono avere rilevanza anche procedimentale e pertanto devono essere conservate per la durata prevista dalla normativa vigente.

Si informa che il Comune 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 dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail. In caso di assenza improvvisa e prolungata del dipendente ovvero per imprescindibili esigenze organizzative e produttive ovvero per motivi di sicurezza del sistema informatico, il Comune, tramite l'Amministratore di Sistema, potrà accedere all'account di posta elettronica dell'Utente secondo la procedura di cui all'art. 11 del presente Regolamento, prendendo visione dei messaggi e dei relativi allegati.

Le informazioni eventualmente raccolte sono altresì utilizzabili per tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, considerato che il presente Regolamento costituisce adeguata informazione sulle modalità d'uso degli strumenti e sulla effettuazione dei controlli ai sensi del GDPR.

Dopo la cessazione del rapporto di lavoro, il back-up dei messaggi di posta elettronica degli Utenti e dei relativi allegati verrà conservato per il periodo di 1 (un) mese.

8. UTILIZZO DI APPARATI DI TELEFONIA, FAX, FOTOCOPIATRICI, SCANNER E STAMPANTI

8.1 Finalità lavorative nell'utilizzo degli apparati di telefonia e di stampa

Gli apparati di telefonia e gli strumenti di stampa sono di proprietà del Comune, possono essere utilizzati solo per finalità collegate all'attività lavorativa svolta dall'Utente per il Comune e devono essere custoditi con diligenza.

Con riferimento a tutti gli apparati telefonici, fermo restando quanto sopra già disposto circa il loro uso e custodia, la ricezione o l'effettuazione di telefonate personali, così come l'invio o la ricezione di SMS o MMS di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa, viene consentita solo nel caso di comprovata necessità ed urgenza.

Le disposizioni del presente paragrafo vanno applicate anche alle sole schede SIM e similari, per quanto compatibili.

Qualora venisse assegnato all'Utente un cellulare del Comune, l'Utente sarà responsabile del suo utilizzo e della sua custodia. Ai cellulari e smartphone del Comune si applicano le medesime regole sopra previste per gli altri dispositivi informatici, per quanto concerne il mantenimento di un adeguato livello di sicurezza informatica nonché le regole per la corretta navigazione in internet.

In caso di smartphone, è vietata l'installazione e l'utilizzo di Applicazioni ("App") diverse da quelle autorizzate dal capo ufficio.

E' vietato l'utilizzo delle fotocopiatrici per fini personali, salvo autorizzazione del Responsabile dell'Ufficio.

Per quanto riguarda l'uso delle stampanti, gli Utenti sono tenuti a:

- stampare documenti solo se strettamente necessari per lo svolgimento delle proprie mansioni lavorative;

- prediligere le stampanti di rete condivise, rispetto a quelle locali, per ridurre l'utilizzo dei materiali di consumo;

- prediligere la stampa in bianco/nero e fronte/retro, al fine di ridurre i costi, se possibile.

- spegnere le stampanti e le fotocopiatrici la sera, prima di lasciare gli uffici.

Nel caso in cui si dovesse stampare documenti contenenti informazioni riservate, l'Utente dovrà presidiare il dispositivo di stampa per evitare la possibile perdita o divulgazione di informazioni a persone terze non autorizzate

8.2 Password

Al fine di evitare accessi od utilizzi impropri o illeciti, tutti i dispositivi di telefonia che lo consentono devono essere protetti da password all'accensione. Quando questo non è possibile, il dispositivo deve essere protetto con l'utilizzo di un PIN.

8.3 Informazioni sulla conservazione dei dati

I dati relativi al traffico telefonico transitato attraverso il centralino del Comune sono conservati per la durata di 1 (un) mese dalle singole comunicazioni, fermo restando la conservazione dei predetti dati da parte degli operatori di telefonia per la durata prevista dalla legge.

9. OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY E DELLA L. 300/1970

Gli strumenti tecnologici considerati nel presente Regolamento costituiscono tutti strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa, anche ai sensi e per gli effetti dell'art. 4, comma secondo, della Legge n. 300/1970. Conseguentemente, le informazioni raccolte sulla base di quanto indicato nel Regolamento, anche conformemente all'articolo successivo, possono essere utilizzate per tutti i fini connessi al rapporto di lavoro, essendone stata data informazione ai lavoratori sulle modalità di uso degli strumenti stessi, sugli interventi che potranno venir compiuti nel sistema informatico aziendale ovvero nel singolo strumento e sui conseguenti sistemi di controllo che potessero venir eventualmente compiuti, fermo restando il rispetto della normativa in materia di protezione dei dati personali (Reg. UE 679/16 e D.lgs. n.196/2003).

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 loro utilizzo come strumenti per il controllo a distanza dell'attività dei lavoratori; peraltro, lì dove l'adozione di tali apparati risultasse necessaria per finalità altre, es. esigenze organizzative e produttive, di sicurezza del lavoro e/o di tutela del patrimonio comunale, il Comune provvederà conformemente a quanto disposto dall'art.4, comma primo, della Legge n. 300/1970, dandone opportuna informazione agli Utenti stessi.

10. ASSISTENZA AGLI UTENTI E MANUTENZIONI

Gli Amministratori di Sistema possono accedere ai dispositivi informatici del Comune sia direttamente, sia mediante software di accesso remoto, per i seguenti scopi:

- verifica e risoluzione di problemi sistemistici ed applicativi, su segnalazione dell'Utente;

- verifica del corretto funzionamento dei singoli dispositivi in caso di problemi rilevati nella rete;

- richiesta di aggiornamento software e manutenzione preventiva hardware e software.

Gli interventi possono avvenire previo consenso dell'Utente, quando l'intervento stesso richiede l'accesso ad aree personali dell'Utente stesso. Qualora l'intervento in loco o in remoto non necessiti di accedere mediante credenziali utente, gli Amministratore di sistema sono autorizzati ad effettuare gli interventi senza il consenso dell'Utente a cui la risorsa è assegnata.

L'accesso in teleassistenza sui PC della rete del Comune richiesto da terzi (fornitori e/o altri) deve essere autorizzato dall'Amministratore di Sistema, per le verifiche delle modalità di intervento per il primo accesso. Le richieste successive, se effettuate con le medesime modalità, possono essere gestite autonomamente dall'Utente. 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.

11. CONTROLLI

11.1 Principi generali

In caso di violazioni contrattuali e giuridiche, sia il Comune che il singolo lavoratore sono potenzialmente perseguibili con sanzioni, anche di natura penale. Per questo motivo il Comune verificherà, nel rispetto delle disposizioni di legge, il rispetto delle regole e l'integrità del proprio sistema informatico.

I controlli dovranno essere adeguati, pertinenti e non eccessivi rispetto alle finalità perseguite ed eseguiti in modo da evitare un'interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori (rispetto dei principi di proporzionalità, trasparenza, pertinenza e non eccedenza).

L'uso degli Apparati e dei Sistemi del Comune può lasciare traccia delle informazioni sul relativo uso, come specificato negli articoli 3, 4, 6, 7 e 8 del presente Regolamento. Tali informazioni, che possono contenere dati personali, anche particolari, riferibili all'Utente, possono essere oggetto di controlli da parte del Comune, tramite l'Amministratore di Sistema, volti a garantire esigenze organizzative e produttive, la sicurezza del lavoro e la tutela del patrimonio del Comune, la sicurezza e salvaguardia del sistema informatico e le ulteriori esigenze tecniche e/o manutentive (ad es. aggiornamento, sostituzione, implementazione di programmi, manutenzione hardware, ecc.). Gli interventi di controllo sono di due tipi, e possono permettere al Comune di prendere indirettamente cognizione dell'attività svolta dagli Utenti.

11.2 Controlli per la tutela del patrimonio del Comune, per la sicurezza e la salvaguardia del sistema informatico. Controlli per ulteriori motivi tecnici e/o manutentivi.

Qualora si renda necessario, per le finalità sopra descritte, di accedere agli Strumenti ed agli Apparati degli Utenti, il Responsabile dell'Ufficio, tramite l'Amministratore di Sistema, si atterrà alla procedura sotto descritta:

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

b) successivamente, almeno dopo 7 (sette) giorni, se il comportamento anomalo persiste, il Comune potrà autorizzare l'Amministratore di Sistema al controllo, potendo così accedere alle informazioni descritte negli articoli 3, 4, 6, 7 e 8, con possibilità di rilevare i file trattati, i 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 il controllo del numero IP dell'Utente e con l'identificazione del soggetto che non si attiene alle istruzioni impartite;

c) qualora il rischio di compromissione del sistema informativo del Comune sia imminente e grave a tal punto da non permettere l'attesa dei tempi necessari per i passaggi procedimentali descritti alle lettere a) e b), il Responsabile dell'Ufficio, unitamente all'Amministratore di Sistema, può intervenire senza indugio sullo strumento da cui proviene la potenziale minaccia.

11.3 Controlli per esigenze produttive e di organizzazione

Per esigenze produttive e di organizzazione si intendono, tra 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, 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 negli articoli 3, 4, 6, 7 e 8, il Responsabile dell'Ufficio, unitamente all'Amministrazione di Sistema, si atterrà alla procedura qui di seguito descritta (se e in quanto compatibile con l'Apparato oggetto di controllo), limitandosi ad accedere ai documenti strettamente indispensabili:

a) redazione da parte del Responsabile dell'Ufficio di un verbale che comprovi le necessità produttive e di organizzazione che richiedono l'accesso allo Strumento;

b) incarico all'Amministratore di Sistema di accedere alla risorsa con credenziali di Amministratore ovvero tramite l'azzeramento e contestuale creazione di nuove credenziali di autenticazione dell'Utente interessato, con avviso che al primo accesso alla risorsa, l'Utente dovrà provvedere alla sostituzione della password;

c) redazione di un verbale che riassuma le operazioni precedenti, sottoscritto dal Responsabile dell'Ufficio e dall'Amministratore di Sistema;

Qualora indirettamente si riscontrino file o informazioni, anche personali, essere potranno essere utilizzabili per tutti i fini connessi al rapporto di lavoro, considerato che il presente Regolamento costituisce adeguata informazione sulle modalità d'uso degli strumenti e sulla effettuazione dei controlli ai sensi del GDPR.

12. CONSERVAZIONE DEI DATI

In riferimento agli articoli 5 e 6 del GDPR 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 o del server proxy), 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. La conservazione dei dati da parte del Comune avverrà nel rispetto di tutte le disposizioni di legge.

13. SANZIONI

È fatto obbligo a tutti gli Utenti di osservare le disposizioni portate a conoscenza con il presente Regolamento. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dalla vigente normativa applicabile, e nei confronti dei collaboratori, consulenti, agenti ed incaricati esterni, verificata la gravità della violazione contestata, con la risoluzione od il recesso dal contratto ad essi relativo nonché con tutte le azioni civili e penali consentite.

14. ENTRATA IN VIGORE

14.1 Il presente Regolamento, che abroga ogni precedente regolamento in materia, entrerà in vigore il giorno in cui diviene esecutiva la relativa delibera di approvazione.

14.2 Il Regolamento verrà pubblicato sul sito internet del Comune, nella sezione Amministrazione Trasparente. Una copia del Regolamento verrà consegnata al Segretario Comunale, ai dipendenti e ai collaboratori del Comune.