COMUNE DI MARINO

Città Metropolitana di Roma Capitale

DISCIPLINARE INTERNO PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI, DI INTERNET, DELLA POSTA ELETTRONICA E DEI SOCIAL NETWORK

Approvato con Delibera Giunta Comunale n. 103 /31.07.2019

Indice dei contenuti

1. SEZIONE I – AMBITO GENERALE

1.1. Definizioni e normativa di riferimento

Il Comune di Marino mette a disposizione del proprio personale e di eventuali collaboratori esterni gli strumenti di lavoro in funzione del ruolo e delle esigenze lavorative:

- strumenti di informatica individuali, quali personal computer e relativi accessori, scanner ecc.
- Apparati e servizi condivisi, quali ad esempio, posta elettronica, Internet, stampanti di rete, server ecc.
- Programmi di produttività individuale e procedure gestionali.

Il presente regolamento illustra le norme generali di utilizzo di tali risorse che il personale e i collaboratori devono rispettare al fine di mitigare I rischi che un uso improprio degli stessi può determinare alla sicurezza del patrimonio informativo e all'immagine dell'Ente nonché l'ambito di eventuali verifiche effettuate dal personale addetto riguardo alla funzionalità e sicurezza dei propri sistemi informativi.

La gestione delle risorse strumentali, ivi incluse quelle informatiche, compete ai singoli Dirigenti di Area.

Nella definizione delle norme comportamentali da osservare si è tenuto conto di quanto previsto dalla normativa vigente in materia dal Regolamento Europeo per la Protezione dei Dati Personali (GDPR)2016/679 e dei provvedimenti emessi dall'Autorità del Garante per la protezione dei dati personali. Tra questi rientrano le "Linee guida del Garante per la posta elettronica e Internet" del 1.03.2017, la circolare AgID 18 aprile 2017 , n. 2/2017.

Il Comune di Marino non effettua registrazioni per il controllo dell'attività lavorativa dei dipendenti, ma solo registrazioni volte a salvaguardare la sicurezza e al mantenimento dell'efficienza dei sistemi. Gli eventuali dati registrati automaticamente a tale scopo non vengono utilizzati in alcun modo per il controllo a distanza dei lavoratori e le tecnologie utilizzate a tal fine sono compatibili con quanto disposto dalla normativa vigente in materia.

1.2. Premessa

L'ambito lavorativo porta il Comune a gestire una serie di "**informazioni**", proprie e di terzi, per poter erogare i servizi che gli vengono contrattualmente richiesti.

Tali informazioni possono essere considerate, ai sensi del GDPR, "**dati personali**" quando sono riferiti a persone fisiche e, per la loro gestione (Trattamento), sia cartaceo che digitale, è necessario che il Comune adotti una serie di adeguate misure tecniche e organizzative atte a proteggere tali dati.

Altre informazioni, pur non essendo "dati personali" ai sensi di legge, sono in tutto e per tutto "**informazioni riservate**", ovvero informazioni tecniche, commerciali, contrattuali, di business o di altro genere per le quali il Comune è chiamato a garantire la riservatezza, o per NDA (accordo di riservatezza), o per una più ampia tutela del patrimonio Comunale.

Ai fini di questo disciplinare si specifica, pertanto, che con il termine "**dati**" deve intendersi l'insieme più ampio di informazioni di cui un soggetto autorizzato (dipendente, collaboratore, tirocinante, …) può venire a conoscenza e di cui deve garantire la riservatezza e la segretezza e non solo i "dati personali" intesi a norma di legge.

Inoltre, nell'ambito della sua attività, il Comune tratta "**dati cartacei**" ovvero informazioni su supporto cartaceo e "**dati digitali**" ovvero informazioni che vengono memorizzate o che semplicemente transitano attraverso apparecchiature digitali.

In linea generale, ogni dato, nell'accezione più ampia sopra descritta, di cui il soggetto autorizzato viene a conoscenza, nell'ambito della propria attività lavorativa, è da considerarsi riservato e non deve essere comunicato o diffuso a nessuno (anche una volta interrotto il rapporto lavorativo con il Comune stesso o qualora parte delle informazioni siano di pubblico dominio) salvo specifica autorizzazione esplicita del Comune.

Anche tra colleghi, oppure tra dipendenti e collaboratori esterni, è necessario adottare la più ampia riservatezza nella comunicazione dei dati conosciuti, limitandosi solo a quei casi che si rendono necessari per espletare al meglio l'attività lavorativa richiesta.

Premesso che i comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, tra i quali rientrano l'utilizzo delle risorse informatiche e telematiche, devono sempre ispirarsi al principio di diligenza e correttezza, il Comune ha adottato il presente Disciplinare diretto a evitare che condotte inconsapevoli possano innescare problemi o minacce alla sicurezza dei dati o delle attrezzature Comunali, esporre potenzialmente l'Ente a possibili rischi di un coinvolgimento di rilevanza sia civile, sia penale, sia amministrativa, creando problemi alla sicurezza e all'immagine del Comune stesso.

Una gestione dei dati cartacei, un uso dei Device Comunali nonché dei servizi di internet e della posta elettronica difforme dalle regole contenute nel presente Disciplinare potrebbe esporre il Comune ad aumentare la minaccia di accessi non autorizzati ai dati e/o al sistema informatico Comunale, furti o divulgazioni di informazioni riservate nonché furti o danneggiamenti del sistema informatico e/o malfunzionamenti in generale dell'intero sistema informatico.

Il presente Disciplinare si applica ai **Soggetti autorizzati** che si trovino ad operare con dati del Comune.

Le informazioni contenute nel presente Disciplinare vengono rilasciate anche ai sensi dell'art. 13 del GDPR e costituiscono, quindi, parte integrante dell'informativa rilasciata ai Soggetti autorizzati.

1.3. Esclusione all'uso degli strumenti informatici

Alla luce del Provvedimento del Garante 1° marzo 2007 che indica di ridurre a titolo cautelativo e preventivo l'utilizzo degli strumenti informatici in considerazione dei pericoli e delle minacce alle quali si è fatto cenno, è fatto esplicito divieto ai soggetti non autorizzati di accedere agli strumenti informatici Comunali.

I casi di esclusione possono riguardare:

1. l'utilizzo del COMPUTER o di altri DEVICE;

2. l'utilizzo della posta elettronica;
3. l'accesso a internet.

Le eventuali esclusioni sono strettamente connesse al principio della natura aziendale e lavorativa degli strumenti informatici nonché al principio di necessità di cui al GDPR. Più specificatamente hanno diritto all'utilizzo degli strumenti e ai relativi accessi solo i soggetti autorizzati che, per funzioni lavorative, ne abbiano un effettivo e concreto bisogno.

I casi in cui le esclusioni dovranno risultare operative in forza di tali motivazioni verranno comunicati individualmente e potranno riguardare sia tutti i casi sopra descritti, sia solo uno o due degli stessi.

1.4. Titolarità dei device e dei dati

Il Comune è esclusivo titolare e proprietario dei Device messi a disposizione ai Soggetti autorizzati ai soli fini dell'attività lavorativa.

Il Comune è l'unico esclusivo titolare e proprietario di tutte le informazioni, le registrazioni ed i dati contenuti e/o trattati mediante i propri device digitali o archiviati in modo cartaceo nei propri locali.

Il soggetto autorizzato non può presumere o ritenere che le informazioni, le registrazioni ed i dati da lui trattati o memorizzati nei device Comunali (inclusi i messaggi di posta elettronica e/o chat inviati o ricevuti, i file di immagini, i files di filmati o altre tipologie di files) siano privati o personali, né può presumere che dati cartacei in suo possesso possano essere da lui copiati, comunicati o diffusi senza l'autorizzazione del Comune.

1.5. Finalità nell'utilizzo dei device

I device assegnati sono uno strumento lavorativo nelle disponibilità del Soggetto autorizzato esclusivamente per un fine di carattere lavorativo. I device, quindi, non devono essere utilizzati per finalità private e diverse da quelle Comunali, se non eccezionalmente e nei limiti evidenziati dal presente Disciplinare.

Qualsiasi eventuale tolleranza da parte di questo Comune, apparente o effettiva, non potrà, comunque, legittimare comportamenti contrari alle istruzioni contenute nel presente Disciplinare.

1.6. Restituzione dei device

A seguito di una cessazione del rapporto lavorativo o di consulenza del Soggetto autorizzato con il Comune o, comunque, al venir meno, a insindacabile giudizio del Comune, della permanenza dei presupposti per l'utilizzo dei device Comunali, i soggetti autorizzati hanno i seguenti obblighi:

1. procedere immediatamente alla restituzione dei device in uso;
2. divieto assoluto di cancellare o formattare o alterare o manomettere o distruggere i device assegnati o rendere inintelligibili i dati in essi contenuti tramite qualsiasi processo, compresa la cifratura dei dati.

1.7. Restituzione dei dati cartacei

A seguito di una cessazione del rapporto lavorativo o di consulenza del Soggetto autorizzato con il Comune o, comunque, al venir meno, a insindacabile giudizio del Comune, della permanenza dei presupposti per l'utilizzo di dati cartacei comunali, i soggetti autorizzati hanno i seguenti obblighi:

1. procedere immediatamente alla restituzione dei dati cartacei in loro possesso;
2. divieto assoluto di cancellare o alterare o manomettere o distruggere i dati cartacei assegnati o renderli inintelligibili tramite qualsiasi processo.

SEZIONE II – PASSWORD

1.8. Le Password

Le password possono essere un metodo di autenticazione assegnato dal Comune per garantire l'accesso protetto a uno strumento hardware oppure a un applicativo software.

La prima caratteristica di una password è la segretezza, e cioè il fatto che non venga svelata ad altri soggetti. La divulgazione delle proprie password o la trascuratezza nella loro conservazione può causare gravi danni al proprio lavoro, a quello dei colleghi e del Comune nel suo complesso. Nel tempo anche la password più sicura perde la sua segretezza. Per questo motivo è buona norma cambiarla con una certa frequenza.

Il Comune ha implementato alcuni meccanismi che permettono di aiutare e supportare i Soggetti autorizzati in una corretta gestione delle password, in particolare, per quanto riguarda le password di accesso al Dominio (ove previsto), è in funzione un sistema automatico di richiesta di aggiornamento delle stesse impostato dal Comune secondo il livello di sicurezza richiesto dal Comune stesso e, comunque, in linea con quanto richiesto dalla valutazione dei rischi effettuata dal Comune in base alle richieste del GDPR.

Altra buona norma è quella di non memorizzare la password su supporti facilmente intercettabili da altre persone. Il miglior luogo in cui conservare una password è la propria memoria.

Le password che non vengono utilizzate da parte degli soggetti autorizzati per un periodo superiore ai sei mesi verranno disattivate dal Comune.

In qualsiasi momento il Comune si riserva il diritto di revocare al Soggetto autorizzato il permesso di accedere a un sistema hardware o software a cui era precedentemente autorizzato, rimuovendo user id o modificando/cancellando la password ad esso associata.

1.9. Regole per la corretta gestione delle password

Il Soggetto autorizzato, da parte sua, per una corretta e sicura gestione delle proprie password deve rispettare le regole seguenti:

1. Le password sono assolutamente personali e non vanno mai comunicate ad altri;
2. Occorre cambiare immediatamente una password non appena si abbia alcun dubbio che sia diventata poco "sicura";
3. Le password devono essere lunghe almeno 8 caratteri e devono contenere anche lettere maiuscole, caratteri speciali[1] e numeri;
4. Le password non devono essere memorizzate su alcun tipo di supporto quali, ad esempio, Post-It (sul monitor o sotto la tastiera) o agende (cartacee, posta elettronica, telefono cellulare);
5. Le password devono essere sostituite almeno nei tempi indicati dalla normativa, a prescindere dall'esistenza di un sistema automatico di richiesta di aggiornamento password **e preferibilmente ogni tre mesi.**
6. Evitare di digitare la propria password in presenza di altri soggetti che possano vedere la tastiera, anche se collaboratori o dipendenti del Comune.
7. Alcuni sistemi (come per esempio la gestione di posta elettronica in uso al momento della redazione del presente disciplinare –Zimbra-) possono prevedere che, in caso di più tentativi errati per l'inserimento della password, bloccano l'account per alcuni minuti meccanismi (nel caso di Zimbra **5** accessi non riusciti consecutivi e **2 minuti di intervello** entro cui devono verificarsi gli accessi non riusciti). In questo caso il soggetto autorizzato deve contattare il Responsabile dei Sistemi Informativi comunale.

[1] Per caratteri speciali si intendono, per esempio, i seguenti: { } [ ] , . < > ; : ! " £ $ % & / ( ) = ? ^ \ | ' * - + _.

1.10. Divieto di uso

Al fine di una corretta gestione delle password, il Comune stabilisce il divieto di utilizzare come propria password:

1. Nome, cognome e loro parti;
2. Lo username assegnato;
3. Un indirizzo di posta elettronica (e-mail);
4. Parole comuni (in Inglese e in Italiano);
5. Date, mesi dell'anno e giorni della settimana, anche in lingua straniera;
6. Parole banali e/o di facile intuizione, ad es. pippo, security e palindromi (simmetria: radar);
7. Ripetizioni di sequenze di caratteri (es. abcabcabc);
8. Una password già impiegata in precedenza.

1.10.1. Alcuni esempi di password non ammesse

La password ideale deve essere complessa, senza alcun riferimento, ma facile da ricordare. Una possibile tecnica è usare sequenze di caratteri prive di senso evidente, ma con singoli caratteri che formano una frase facile da memorizzare (es.: "NlMzz5DlCmm!", Nel Mezzo Del Cammin, più il carattere 5 e il punto esclamativo). Decifrare una parola come questa può richiedere giorni, una come "radar" meno di dieci secondi. Alcuni esempi di password assolutamente da evitare:

1. Se Username = "mariorossi", password = "mario", o ancora peggio, password = "mariorossi";
2. Il nome della moglie/marito, fidanzato/a, figli, ecc...anche a rovescio!;
3. La propria data di nascita, quella del coniuge, ecc.;
4. Targa della propria auto;
5. Numero di telefono proprio, del coniuge, ecc.;
6. Parole comuni tipo "Kilimangiaro", "Password", "Qwerty", "12345678" (troppo facili);
7. Qualsiasi parola del vocabolario (di qualsiasi lingua diffusa, come inglese, italiano, ecc.).

1.11. La password nei sistemi

Ogni Soggetto autorizzato può variare la propria password di accesso a qualsiasi sistema Comunale in modo autonomo, qualora il sistema in questione metta a disposizione degli Utenti una funzionalità di questo tipo (Change password), oppure facendone richiesta al Titolare. La password può essere sostituita dal Titolare, anche qualora l'Utente l'abbia dimenticata.

SEZIONE III – OPERAZIONI A PROTEZIONE DELLA POSTAZIONE DI LAVORO.

In questa sezione vengono trattate le operazioni a carico del Soggetto autorizzato e il quadro di riferimento generale per l'esecuzione di operazioni a protezione della propria postazione di lavoro, nel rispetto della sicurezza e dell'integrità del patrimonio Comunale.

1.12. Login e Logout

Il "Login" è l'operazione con la quale il Soggetto autorizzato si connette al sistema informativo Comunale o a una parte di esso, dichiarando il proprio Username e Password (ossia l'Account), aprendo una sessione di lavoro. In molti casi è necessario effettuare più login, tanti quanti sono gli ambienti di lavoro (ad es. applicativi web, Intranet), ognuno dei quali richiede un username e una password.

In questi casi, sebbene sia preferibile che ogni utente abbia un suo specifico user name e password, il Comune potrà assegnare un univoco user name e password per gruppi di soggetti autorizzati per l'accesso alla macchina fisica, mentre rimarranno separati ed univoci per l'accesso agli applicativi che contengono dati.

Il "Logout" è l'operazione con cui viene chiusa la sessione di lavoro. Al termine della giornata lavorativa, tutte le applicazioni devono essere chiuse secondo le regole previste dall'applicazione stessa. La non corretta chiusura può provocare una perdita di dati o l'accesso agli stessi da parte di persone non autorizzate.

1.13. Obblighi

L'utilizzo dei dispositivi fisici e la gestione dei dati ivi contenuti devono svolgersi nel rispetto della sicurezza e dell'integrità del patrimonio dati Comunale.

Il soggetto autorizzato deve quindi eseguire le operazioni seguenti:

1. Se si allontana dalla propria postazione dovrà mettere in protezione il suo device affinché persone non autorizzate non abbiano accesso ai dati protetti oppure ogni qualvolta abbia bisogno di allontanarsi dalla propria postazione, per esempio, bloccando autonomamente il pc per poi riattivarlo inserendo la propria password (per bloccare: control + alt+ canc);
2. Chiudere la sessione (Logout) a fine giornata;
3. Spegnere il PC dopo il Logout;
4. Controllare sempre che non vi siano persone non autorizzate alle sue spalle che possano prendere visione delle schermate del suo device.

2. SEZIONE IV - USO DEL PERSONAL COMPUTER DEL COMUNE

2.1. Modalità d'uso del COMPUTER Comunale

Il sistema informativo Comunale è composto da un insieme di unità server centrali e macchine client connessi ad una rete locale (LAN), che utilizzano diversi sistemi operativi e applicativi.

I files creati, elaborati o modificati sul computer assegnato devono essere poi sempre salvati a fine giornata sul sistema di repository documentale centralizzato. Il Comune non effettua il backup dei dati memorizzati in locale.

2.2. Corretto utilizzo del COMPUTER Comunale

Il computer consegnato al soggetto autorizzato è uno strumento di lavoro e contiene tutti i software necessari a svolgere le attività affidate. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, rallentamenti del sistema, costi di manutenzione e, soprattutto, minacce alla sicurezza.

L'accesso all'elaboratore è protetto da password che deve essere custodita dal soggetto autorizzato con la massima diligenza e non divulgata. Il computer che viene consegnato contiene tutti i software necessari a svolgere le attività affidate dal Comune. Per necessità Comunali, gli amministratori di sistema utilizzando la propria login con privilegi di amministratore e la password dell'amministratore, potranno accedere, con le regole indicate nel presente documento, sia alla memoria di massa locali di rete (repository e backup) che ai server Comunali nonché, previa comunicazione al dipendente, accedere al computer, anche da remoto.

In particolare il Soggetto autorizzato deve adottare le seguenti misure:

1. utilizzare solo ed esclusivamente le aree di memoria della rete del Comune ed ivi creare e registrare file e software o archivi dati, senza pertanto creare altri files fuori dalle unità di rete;

2. spegnere il computer, o curarsi di effettuare il Logout, ogni sera prima di lasciare gli uffici o in caso di assenze prolungate, poiché lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso;
3. mantenere sul computer esclusivamente i dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori), disposti dal Comune;
4. Non dare accesso al proprio computer ad altri utenti, a meno che siano soggetti autorizzati con cui condividono l'utilizzo dello stesso Pc o a meno di necessità stringenti e sotto il proprio costante controllo.

2.3. Divieti Espressi sull'utilizzo del COMPUTER

All'soggetto autorizzato è vietato:

1. La gestione, la memorizzazione (anche temporanea) o il trattamento di file, documenti e/o informazioni personali del soggetto autorizzato o comunque non afferenti alle attività lavorative nella rete, nel disco fisso o in altre memorie di massa Comunali e negli strumenti informatici Comunali in genere.
2. Modificare le configurazioni già impostate sul personal computer.
3. Utilizzare programmi e/o sistemi di criptazione senza la preventiva autorizzazione scritta del Comune.
4. Installare alcun software di cui il Comune non possieda la licenza, né installare alcuna versione diversa, anche più recente, rispetto alle applicazioni o al sistema operativo presenti sul personal computer consegnato, senza l'espressa autorizzazione del Comune. Né è, peraltro, consentito fare copia del software installato al fine di farne un uso personale.
5. Caricare sul disco fisso del computer o nel server alcun documento, gioco, file musicale o audiovisivo o immagine diversi da quelli necessari allo svolgimento delle mansioni affidate.
6. Aggiungere o collegare dispositivi hardware (ad esempio hard disk, driver, PCMCIA, ecc.) o periferiche (telecamere, macchine fotografiche, smartphone, chiavi USB ecc.) diversi da quelli consegnati, senza l'autorizzazione espressa del Comune.
7. Creare o diffondere, intenzionalmente o per negligenza, programmi idonei a danneggiare il sistema informatico del Comune, quali per esempio virus, trojan horses ecc.
8. Accedere, rivelare o utilizzare informazioni non autorizzate o comunque non necessarie per le mansioni svolte.
9. Effettuare in proprio attività manutentive.
10. Permettere attività manutentive da parte dei soggetti non espressamente autorizzati del Comune.

2.4. ANTIVIRUS

I virus possono essere trasmessi tramite scambio di file via internet, via mail, scambio di supporti removibili, filesharing, chat, via mail …

Il Comune impone su tutte le postazioni di lavoro l'utilizzo di un sistema antivirus correttamente installato, attivato continuamente e aggiornato automaticamente con frequenza almeno quotidiana.

Il soggetto autorizzato, da parte sua, deve impegnarsi a controllare il corretto funzionamento e aggiornamento del sistema antivirus installato sul proprio computer, e, in particolare, deve rispettare le regole seguenti:

1. Comunicare al Comune ogni anomalia o malfunzionamento del sistema antivirus;
2. Comunicare al Comune eventuali segnalazioni di presenza di virus o file sospetti.

Inoltre, al soggetto autorizzato:

1. È vietato accedere alla rete Comunale senza servizio antivirus attivo e aggiornato sulla propria postazione;
2. È vietato ostacolare l'azione dell'antivirus Comunale;
3. È vietato disattivare l'antivirus senza l'autorizzazione espressa del Comune e anche e soprattutto nel caso sia richiesto per l'installazione di software sul computer;
4. È vietato aprire allegati di mail provenienti da mittenti sconosciuti o di dubbia provenienza o allegati di mail di persone conosciute ma con testi inspiegabili o in qualche modo strani.

Contattare il responsabile dei sistemi informativi prima di procedere a qualsiasi attività potenzialmente in conflitto con quanto sopra.

5. SEZIONE V – INTERNET

1.5 Internet è uno strumento di lavoro

La connessione alla rete internet dal device avuto in dotazione è ammessa esclusivamente per motivi attinenti allo svolgimento dell'attività lavorativa. L'utilizzo per scopi personali è limitatamente consentito previa autorizzazione e con gli accorgimenti di cui al presente documento.

Solo il personale autorizzato può accedere, dai device istituzionali in dotazione, ai Social Network Istituzionali e a quelli d'interesse collegato.

2.5. Misure preventive per ridurre navigazioni illecite

Il Comune potrà adottare idonee misure tecniche preventive volte a ridurre navigazioni a siti non correlati all'attività lavorativa attraverso filtri e black list implementati ad esempio attraverso i sistemi di content filter dei firewall.

2.6. Divieti Espressi concernenti Internet

1. È vietata la navigazione nei siti che possono rivelare le opinioni politiche religiose, sindacali e di salute dell'Soggetto autorizzato poiché potenzialmente idonea a rivelare dati personali ai sensi del GDPR.
2. È fatto divieto di accedere a siti internet che abbiano un contenuto contrario a norme di legge e a norme a tutela dell'ordine pubblico, rilevante ai fini della realizzazione di una fattispecie di reato o che siano in qualche modo discriminatori sulla base della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, degli handicap.
3. È vietato al Soggetto autorizzato lo scarico di software (anche gratuito) prelevato da siti Internet;
4. È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dal Titolare e con il rispetto delle normali procedure di acquisto.
5. È vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.
6. È vietata la partecipazione a forum non professionali, l'utilizzo di chat line, di bacheche elettroniche o partecipare a gruppi di discussione o lasciare commenti ad articoli o iscriversi a mailing list spendendo il marchio o la denominazione del Comune, salvo specifica autorizzazione del Comune stessa.
7. È vietata la memorizzazione di documenti informatici di natura oltraggiosa, diffamatoria e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
8. È vietato al Soggetto autorizzato di promuovere utile o guadagno personale attraverso l'uso di Internet o della posta elettronica Comunale.
9. È vietato accedere dall'esterno alla rete interna del Comune, salvo specifica autorizzazione e con le specifiche procedure previste dal Comune stesso.
10. È vietato, infine, creare siti web personali sui sistemi del Comune nonché acquistare beni o servizi su Internet a meno che l'articolo acquistato non sia stato approvato a titolo di spesa professionale.

11. È vietato utilizzare internet per attività di file sharing.
12. E' vietato navigare su siti privati previa autorizzazione del Dirigente Sistemi Informativi.

Ogni eventuale navigazione rientrante nel punto 3.3., comportando un illegittimo utilizzo di Internet nonché un possibile illecito trattamento di dati personali e sensibili, è posta sotto la personale responsabilità del Soggetto autorizzato inadempiente e può dar luogo a provvedimenti disciplinari secondo quanto previsto dal CCNL adottato dal Comune.

2.7. Divieti di Sabotaggio

È vietato accedere ad alcuni siti internet mediante azioni inibenti dei filtri, sabotando o comunque superando o tentando di superare o disabilitando i sistemi adottati dal Comune per bloccare accessi non conformi all'attività lavorativa. In ogni caso è vietato utilizzare siti o altri strumenti che realizzino tale fine.

2.8. Diritto d'autore

È vietato utilizzare l'accesso ad Internet in violazione delle norme in vigore nell'ordinamento giuridico italiano a tutela del diritto d'autore (es. legge 22 aprile 1941, n. 633 e successive modificazioni, 6 maggio 1999, n. 169 e legge 18 agosto 2000, n. 248 e s.m.i.). In particolare, è vietato il download di materiale soggetto a copyright (testi, immagini, musica, filmati, file in genere, …) se non espressamente autorizzato dal Comune.

6 SEZIONE VI: SOCIAL NETWORK COMUNALI- APPLICAZIONI GRATUITE UTILIZZATE DAI CITTADINI

L'utilizzo dei Social Media ha da qualche tempo una funzione istituzionale molto importante e notevolmente impattante sull'immagine e la qualità percepita dell'Amministrazione.

Proprio per questo motivo ci sono alcune regole di base che devono essere rispettate, in alcuni casi perfino ovvie. I profili ufficiali istituzionali all'interno del Social Network devono presentare il logo Comunale, il sito Internet ufficiale a rappresentare ai terzi il carattere istituzionale ed ufficiale della pagina ed individuare in maniera univoca l'identità, in alcuni casi anche il Servizio Referente. Nelle informazioni generali occorre descrivere la mission Comunale. Al momento della redazione del presente documento sono attivi per il Comune di Marino i seguenti profili social:

 Comune di Marino  comunemarino  @ComuneMarino  COMUNE DI MARINO

Nei profili social è riportata la posta elettronica dell'ufficio responsabile per eventuali segnalazioni e reclami in materia di violazione di copyright, privacy, furti di identità, reati informatici ed eventuali disservizi.

L'Amministratore / Amministratori e il Redattore/ Redattori dei comunicati istituzionali che vengono pubblicati nelle pagine Social sono nominati dall'Ente con atto deliberativo. Se è previsto un moderatore/admin che rappresenta la voce ufficiale del Comune sulle pagine Social deve essere chiaramente indicato e non può essere rappresentato da altri soggetti, dipendenti o collaboratori del Comune che dovessero intervenire sulla pagina.

Gli amministratori ed eventuali moderatori devono attenersi a precise regole ed istruzioni nel rigoroso rispetto della normativa privacy e del Disciplinare. Il Comune ribadisce la natura istituzionale e Comunale dello spazio sui Social Network attraverso le modalità di linguaggio e di intervento e di ingaggio utilizzate dagli amministratori e moderatori (se nominati).

La Social Media Policy ad uso esterno tramite le piattaforme Social

Nella individuazione delle regole di netiquette da seguire all'interno del prezioso spazio di interazione e dialogo del Social Network in linea con le condizioni generali di utilizzo dello stesso (ad esempio: https://www.facebook.com/legal/terms), si dovrà precisare che il Comune non è responsabile dei commenti e dei contenuti pubblicati sulle pagine Social Comunali dagli utenti e che il Comune ha il diritto di rimuovere, anche senza preavviso e a propria discrezione, dalle pagine comunali del Social Media qualunque commento, in particolare i commenti e i materiali offensivi, volgari, classificabili come istigazione alla violenza, all'intolleranza e alla discriminazione ovvero in violazione del diritto alla protezione di dati personali (privacy), copyright, marchi, diritto all'immagine e della relativa privacy policy adottata.

Il Comune specifica che può bloccare e segnalare al Social Media interessato gli utenti che hanno infranto la policy e nei casi più gravi ricorrere alla Polizia Postale

In riferimento al diritto alla protezione dei dati personali il Comune specifica e avverte gli utenti in modo semplice e diretto della possibilità che i dati, le informazioni, i commenti postati possono essere indicizzati dai motori di ricerca generalisti ed essere conosciuti senza limiti di tempo e di spazio dalla generalità degli utenti di internet e non dai soli iscritti alla pagina Comunale.

Richiamata la propria privacy policy del sito Comunale è opportuno illustrare agli utenti l'utilizzo o meno di cookies specificando che il Comune tratta i dati visibili degli utenti sulla piattaforma on line esclusivamente ai fini istituzionali e per il tempo strettamente necessario per il perseguimento di tale finalità.

L'amministratore delle piattaforme social, pur potendo vedere dati specifici pertinenti alla fruizione dei servizi da parte degli utenti social, non può trattare ulteriormente tali dati per finalità diverse da quelle specificate dalle policy privacy contenute nelle piattaforme social. Tale divieto è tassativo al fine di evitare sanzioni da parte delle autorità preposte (Garante della privacy), anche alla luce delle recenti sentenze che hanno colpito sul tema diversi operatori economici (giugno 2018, sentenza della Corte Europea di Lussemburgo, sul caso della società tedesca Wirtschaftsakademie)

Il Comune inserisce alcune regole di comportamento nelle operazioni di caricamento di fotografie e video da parte degli utenti e specifica che gli stessi devono acquisire il consenso delle persone ritratte. In riferimento al diritto di autore, si specifica che i materiali pubblicati dal Comune, all'interno dello spazio Social, qualora non diversamente indicato, sono di proprietà del Comune e coperti da copyright; il Comune richiede agli utenti di prestare molta attenzione all'utilizzo dei contenuti, video, musica, foto, materiali di terzi soggetti coperti dal copyright e segnala agli stessi di non pubblicare materiali coperti da copyright senza la relativa autorizzazione e raccomanda agli utenti di caricare i contenuti, musiche, video rilasciati con licenze creative commons, in quanto utilizzabili liberamente e gratuitamente al fine di non esporre il Comune ad eventuale contenzioso (es. chiusura dello stesso profilo sul Social Network). Il Comune specifica come compia ogni sforzo possibile per migliorare il livello di completezza e aggiornamento delle informazioni e dei contenuti. Il Comune specifica agli utenti in modo semplice e trasparente gli eventuali soggetti all'interno del Comune (administrator; moderatore qualora nominati) autorizzati a rispondere in via ufficiale ai commenti postati on line (principio dell'affidamento esterno). Inoltre il Comune rappresenta agli utenti che non è in alcun modo responsabile della mancata fruizione della piattaforma on line o dei relativi collegamenti alla piattaforma on line.

I termini di servizio

Se è vero che, nella gran parte dei casi, l'iscrizione a un sito di Social Networking è gratuita, è anche vero che la registrazione di un profilo comporta la conclusione di un vero e proprio contratto a oggetto informatico (cosiddetto contratto di Social Networking). Al soggetto autorizzato dal Comune alla gestione dei Social Network che avviene tramite apposita delibera, viene fornito uno specifico account Comunale. Non sono consentite pagine Comunali gestite tramite account personali. Il Comune si riserva di consentire l'accesso alle piattaforme social per mezzo di dispositivi Comunali, gestiti e prestabiliti. Assume grande importanza la lettura dei termini

di servizio (in inglese Terms of Service o TOS) che devono essere accettati dall'utente prima di poter accedere ai servizi di Social Media e, quindi, prima della creazione del profilo. Tali condizioni, che è opportuno conservare al pari di qualunque altro contratto, si occupano di:

- riservatezza dei dati degli utenti (privacy policy);
- condotte consentite all'utente;
- diritti sui contenuti inseriti dagli utenti;
- limitazioni di responsabilità del fornitore.

Tra gli aspetti maggiormente rilevanti rientrano quelli legati alla riservatezza degli utenti e ai contenuti veicolati attraverso i canali sociali. Con riferimento al primo aspetto, deve essere sempre garantita la conformità con quanto previsto dal codice in materia di protezione dei dati personali (D.Lgs. n. 196/2003 e s.m.i.) e dal GDPR; invece, in relazione ai diritti d'autore e di proprietà intellettuale che il Comune può vantare su alcuni dei contenuti pubblicati, si deve tenere conto che alcuni provider nei propri modelli contrattuali prevedono che l'utente trasferisca al fornitore il diritto di utilizzare, anche a fini commerciali, il materiale ospitato sui propri server. Inoltre, bisogna prestare attenzione al tipo di comportamenti vietati dal gestore del Social Network che possono comportare la cancellazione del profilo o dell'account del Comune e alla circostanza che tutti i contenuti pubblicati sui canali Social non possano ledere i diritti d'autore o di proprietà intellettuale di terzi soggetti; tale comportamento potrebbe vanificare gli investimenti effettuati, oltre danneggiarne l'immagine ed esporla a contenzioso. Inoltre, dal momento che i termini di servizio sono soggetti a frequente revisione e modifica da parte dei fornitori del servizio stesso, è opportuno monitorarne l'evoluzione in modo da valutare, volta per volta, se le modifiche possano essere accettate oppure il Comune debba abbandonare il Social Network.

Aggiornamento periodico

La velocità dei mutamenti e l'eterogeneità dei Social Network (in genere le strategie di Social Networking ne ricomprendono molteplici: Twitter, Facebook, LinkedIn, Instagram …), impone un'assidua osservazione delle policy, dei contratti e, a cascata, delle linee guida Comunali che su di essi possono essere strutturate.

UTILIZZO DI APPLICAZIONI GRATUITE

Nel caso si utilizzino applicazioni gratuite (tipo Municipium) per fornire servizi ai cittadini quali la possibilità d'inviare segnalazioni/disservizi/suggerimenti che comportano cessione di dati personali/dati sensibili il Comune deve nominare i responsabili del trattamento di eventuali dati personali /sensibili. Tali dati devono essere utilizzati ai soli fini istituzionali per gestire le segnalazioni/disservizi/suggerimenti. I responsabili nominati dovranno attenersi alle normative vigenti in materia di privacy.

7. SEZIONE VII – POSTA ELETTRONICA

a. La Posta Elettronica è uno strumento di lavoro

L'utilizzo della posta elettronica Comunale è connesso allo svolgimento dell'attività lavorativa. L'uso per motivi personali deve essere moderato ed è tollerato esclusivamente ai sensi dell'articolo seguente.

I Soggetti autorizzati possono avere in utilizzo indirizzi nominativi di posta elettronica.

Le caselle e-mail possono meglio essere assegnate con natura impersonale (tipo info, amministrazione, fornitori, direttore, direttore sanitario, consulenza, …) proprio per evitare

ulteriormente che il destinatario delle mail possa considerare l'indirizzo assegnato al dipendente "privato", ai sensi dei suggerimenti del Garante a tal proposito.

I Soggetti autorizzati assegnatari delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

b. Misure Preventive per ridurre utilizzi illeciti della Posta Elettronica

Il Comune è consapevole della possibilità di un limitato utilizzo personale della posta elettronica da parte dei Soggetti autorizzati e allo scopo prevede le seguenti misure:

1. In caso di ricezione sulla e-mail Comunale di posta personale si avverte di cancellare immediatamente ogni messaggio al fine di evitare ogni eventuale e possibile back up dei dati.
2. Avvisare il Comune quando alla propria posta personale siano allegati files eseguibili e/o di natura incomprensibile o non conosciuta.

c. Divieti Espressi

1. È vietato utilizzare l'indirizzo di posta elettronica contenente il dominio del Comune per iscriversi in qualsivoglia sito per motivi non attinenti all'attività lavorativa, senza espressa autorizzazione scritta del Comune, nonché utilizzare il dominio dell'Comune per scopi personali.
2. È vietato redigere messaggi di posta elettronica utilizzando l'indirizzo Comunale, diretti a destinatari esterni del Comune, senza utilizzare il seguente disclaimer:

   «Il presente messaggio e gli eventuali suoi allegati sono di natura Comunale, prevalentemente confidenziale e sono visionabili solo dal destinatario di posta elettronica. La risposta o l'eventuale invio spontaneo da parte vostra di e-mail al nostro indirizzo potrebbero non assicurare la confidenzialità potendo essere viste da altri soggetti appartenenti al Comune oltre al sottoscritto, per finalità di sicurezza informatica, amministrative e allo scopo del continuo svolgimento dell'attività Comunale. Qualora questo messaggio vi fosse pervenuto per errore, vi preghiamo di cancellarlo dal vostro sistema e vi chiediamo di volercene dare cortesemente comunicazione al mittente".
3. È vietato creare, archiviare o spedire, anche solo all'interno della rete Comunale, messaggi pubblicitari o promozionali o comunque allegati (filmati, immagini, musica o altro) non connessi con lo svolgimento della propria attività lavorativa, nonché partecipare a richieste, petizioni, mailing di massa di qualunque contenuto, "catene di Sant'Antonio" o in genere a pubblici dibattiti utilizzando l'indirizzo Comunale.
4. È vietato trasmettere messaggi a gruppi numerosi di persone (es. a tutto un ufficio o ad un'intera divisione) senza l'autorizzazione necessaria.
5. È vietato sollecitare donazioni di beneficenza, propaganda elettorale o altre voci non legate al lavoro.
6. È vietato utilizzare il servizio di posta elettronica per trasmettere a soggetti esterni del Comune informazioni riservate o comunque documenti Comunali, se non nel caso in cui ciò sia necessario in ragione delle mansioni svolte.
7. È vietato utilizzare la posta elettronica per messaggi con allegati di grandi dimensioni.

d. Posta Elettronica in caso di assenze programmate ed assenze non programmate

Nel caso di assenza prolungata sarebbe buona norma attivare il servizio di risposta automatica (Auto-reply).

In alternativa e in tutti i casi in cui sia necessario un presidio della casella di e-mail per ragioni di operatività Comunale, il Dirigente preposto può nominare un collega fiduciario del precedente con lettera scritta che in caso di assenza inoltri i files necessari a chi ne abbia urgenza.

Qualora il Soggetto autorizzato non abbia provveduto ad individuare un collega fiduciario o questi sia assente o irreperibile, il Dirigente potrà verificare il contenuto dei messaggi di posta elettronica del soggetto autorizzato, informandone il soggetto autorizzato stesso.

e. Utilizzo Illecito di Posta Elettronica

1. È vietato inviare, tramite la posta elettronica, anche all'interno della rete Comunale, materiale a contenuto violento, sessuale o comunque offensivo dei principî di dignità personale, di libertà religiosa, di libertà sessuale o di manifestazione del pensiero, anche politico.
2. È vietato inviare messaggi di posta elettronica, anche all'interno della rete Comunale, che abbiano contenuti contrari a norme di legge ed a norme di tutela dell'ordine pubblico, rilevanti ai fini della realizzazione di una fattispecie di reato, o che siano in qualche modo discriminatori della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, degli handicap.
3. Qualora il Soggetto autorizzato riceva messaggi aventi tale contenuto, è tenuto a cancellarli immediatamente e a darne comunicazione all'Comune.

8. SEZIONE VIII – USO DI ALTRI DEVICE (PERSONAL COMPUTER PORTATILE, TABLET, CELLULARE, SMARTPHONE E DI ALTRI DISPOSITIVI ELETTRONICI)

a. L'utilizzo del notebook, tablet o smartphone.

Il computer portatile, il tablet e il cellulare (di seguito generalizzati in "device mobile") possono venire concessi in uso dal Comune ai Soggetti autorizzati che durante gli spostamenti necessitino di disporre di archivi elettronici, supporti di automazione e/o di connessione alla rete del Comune.

Il Soggetto autorizzato è responsabile dei device mobili assegnatigli dal Comune e deve custodirli con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Ai device mobili si applicano le regole di utilizzo previste per i computer connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna. In particolare i files creati o modificati sui device mobili devono essere trasferiti sulle memorie di massa Comunali al primo rientro in ufficio e cancellati in modo definitivo dai device mobili (Wiping). Sui device mobili è vietato installare applicazioni (anche gratuite) se non espressamente autorizzate dal Comune. I device mobili utilizzati all'esterno (convegni, ecc…), in caso di allontanamento, devono essere custoditi in un luogo protetto. In caso di perdita o furto dei device mobili deve far seguito la denuncia alle autorità competenti. Allo scopo si deve avvisare immediatamente il Comune che provvederà – se del caso – ad occuparsi delle procedure connesse alla privacy. Anche di giorno, durante l'orario di lavoro, al Soggetto autorizzato non è consentito lasciare incustoditi i device mobili.

Al Soggetto autorizzato è vietato lasciare i device mobili incustoditi e a vista dentro l'auto o in una stanza d'albergo o nell'atrio dell'albergo o nelle sale d'attesa delle stazioni ferroviarie e aeroportuali.

I device mobili che permettono l'attivazione di una procedura di protezione (PIN) devono sempre essere abilitabili solo con la digitazione del PIN stesso e non possono essere lasciti privi di PIN.

Laddove il device mobile sia accompagnato da un'utenza, il Soggetto autorizzato è chiamato ad informarsi preventivamente dei vincoli ad essa associati (es. numero minuti massimo, totale gigabyte dati, …) e a rispettarli. Qualora esigenze lavorative richiedessero requirements differenti l'Soggetto autorizzato è tenuto ad informare tempestivamente e preventivamente al Comune.

In relazione alle utenze mobili, salvo autorizzazione del Comune, è espressamente vietato ogni utilizzo all'estero e anche in caso di autorizzazione del Comune, gli utilizzi all'esterno devono essere preventivamente comunicati al Comune per permettere l'attivazione di opportuni contratti di copertura con l'operatore mobile di riferimento.

Alcuni Device mobili, quali smartphone e tablet, possono essere dotati dal Comune di particolari misure di protezione (MDM o altro).

b. Memorie esterne (chiavi usb, hard disk, memory card, cd-rom, dvd, …)

Ai Soggetti autorizzati può essere assegnata una memoria esterna (quale una chiave USB, un hard disk esterno, una memory card, …) su cui copiare temporaneamente dei dati per un facile trasporto, o altri usi (es. macchine fotografiche con memory card, videocamere con dvd, …).

Questi dispositivi devono essere gestiti con le stesse accortezze di cui all'articolo precedente e devono essere utilizzati esclusivamente dalle persone a cui sono state affidate e, in nessun caso, devono essere consegnate a terzi.

Si sconsiglia l'uso di dischetti, CD-ROM, memorie USB o analoghi supporti di memorizzazione di incerta provenienza che potrebbero causare danni alla postazione di lavoro.

c. Device personali

E' vietato l'utilizzo di memorie esterne personali (quali chiavi USB, memory card, cd-rom, DVD, macchine fotografiche, videocamere, tablet, …), nonché di salvare qualsiasi tipologia di dato su PC che non sono di proprietà Comunali.

Solo se espressamente autorizzati alcuni soggetti/dipendenti possono utilizzare i propri device personali per memorizzare dati del Comune assumendone formalmente e personalmente l'intera responsabilità del trattamento.

Tali device dovranno essere preventivamente valutati dal Comune, per la verifica della sussistenza di adeguate misure di sicurezza.

A tal riguardo, nel caso in cui device personali siano oggetto di perdita, furto o sostituzione sarà compito del soggetto/ dipendente utilizzatore dell'account Comunale comunicare in maniera tempestiva l'accaduto al fine di attivare le conseguenti misure di sicurezza previste (Mobile Device Management – che prevede la cancellazione dei dati Comunali).

d. Utilizzo del cellulare/smartphone personale istituzionale.

Durante l'orario di lavoro, comprese le eventuali pause, ai Soggetti autorizzati è concesso l'utilizzo del telefono cellulare istituzionale solo per comunicazioni di emergenza o strettamente collegate all'ambito lavorativo.

In caso di trasferte lavorative all'esterno, il telefono personale istituzionale deve rimanere acceso nei tempi autorizzati anche per facilitare la comunicazione con il Comune stesso ove fosse necessario.

In ogni caso il telefono istituzionale non deve essere utilizzato per fini personali in particolare in presenza di cittadini o fornitori.

e. Distruzione dei Device

Ogni Device ed ogni memoria esterna affidati ai soggetti autorizzati, (computer, notebook, tablet, smartphone, memory card, chiavi usb, hard disk, dvd, cd-rom, ecc.), al termine del loro utilizzo dovranno essere restituiti al Responsabile Servizi Informatici che provvederà a distruggerli o a ricondizionarli seguendo le norme di legge in vigore al momento.

In particolare il Comune provvederà a cancellare o a rendere inintelligibili i dati negli stessi memorizzati.

9. SEZIONE IX – SISTEMI IN CLOUD

a. Cloud Computing

In informatica con il termine inglese cloud computing (in italiano nuvola informatica) si indica un paradigma di erogazione di risorse informatiche, come l'archiviazione, l'elaborazione o la trasmissione di dati, caratterizzato dalla disponibilità on demand attraverso Internet a partire da un insieme di risorse preesistenti e configurabili.

Le risorse non vengono pienamente configurate e messe in opera dal fornitore apposta per l'utente, ma gli sono assegnate, rapidamente e convenientemente, grazie a procedure automatizzate, a partire da un insieme di risorse condivise con altri utenti lasciando all'utente parte dell'onere della configurazione. Quando l'utente rilascia la risorsa, essa viene similmente riconfigurata nello stato iniziale e rimessa a disposizione nel pool condiviso delle risorse, con altrettanta velocità ed economia per il fornitore.

Utilizzare un servizio di cloud computing per memorizzare dati personali o sensibili, espone il Comune a potenziali problemi di violazione della privacy. I dati personali vengono memorizzati nel server farms di aziende che spesso risiedono in uno stato extraeuropeo, configurando un trasferimento dei dati all'estero. Il cloud provider, in caso di comportamento scorretto o malevolo, potrebbe accedere ai dati personali per eseguire ricerche di mercato e profilazione degli utenti,

Con i collegamenti wireless, il rischio sicurezza aumenta e si è maggiormente esposti ai casi di pirateria informatica a causa della minore sicurezza offerta dalle reti senza fili. In presenza di atti illegali, come appropriazione indebita o illegale di dati personali, il danno potrebbe essere molto grave per il Comune, con difficoltà di raggiungere soluzioni giuridiche e/o rimborsi se il fornitore risiede in uno stato diverso da paese dell'utente.

Nel caso di industrie o aziende, tutti i dati memorizzati nelle memorie esterne sono seriamente esposti a eventuali casi di spionaggio industriale.

b. Utilizzo di sistemi cloud

È vietato ai soggetti autorizzati l'utilizzo di sistemi Cloud non espressamente approvati dal Comune. Per essere approvati i sistemi cloud devono rispondere ad almeno i seguenti requisiti:

- Essere sistemi cloud di cui si conosce l'esatto posizionamento dei server e per i quali si è predisposto quanto richiesto dalle norme, compreso eventualmente quello che è richiesto per il trasferimento dei dati all'estero;
- L'azienda che fornisce il sistema in Cloud deve essere preventivamente nominata Responsabile al Trattamento dei dati da parte del Comune;
- L'azienda che fornisce il sistema in Cloud deve comunicare al Comune, almeno una volta all'anno, i nominativi degli amministratori di sistema utilizzati.
- Dovranno essere verificate tutte le indicazioni e le prescrizioni previste dal Garante della Privacy nei suoi provvedimenti sugli Amministratori di Sistema e sul Cloud.

10. SEZIONE X – GESTIONE DATI CARTACEI

a. Dati cartacei- Policy

I Soggetti autorizzati sono responsabili del controllo e della custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali.

I Soggetti autorizzati sono invitati dal Comune ad adottare una "politica della scrivania pulita". Ovvero si richiede ai soggetti autorizzati di trattare dati cartacei solo se necessario, privilegiando, ove possibile, l'utilizzo degli strumenti digitali messi a disposizione del Comune.

I principali benefici di una politica della scrivania pulita sono:

1) Una buona impressione ai cittadini e fornitori che visitano il Comune;
2) La riduzione della possibilità che informazioni confidenziali possano essere viste da persone non abilitate a conoscerle;
3) La riduzione che documenti confidenziali possano essere sottratti al Comune.

In particolare, si invita a non lasciare in vista sulla propria scrivania dati cartacei quando ci si allontana dalla stessa oppure quando è previsto un incontro con un soggetto non abilitato alla conoscenza dei dati in essi contenuti.

Prima di lasciare la propria postazione (per esempio per la pausa pranzo o per una riunione) sarà cura dei Soggetti autorizzati riporre in luogo sicuro (armadio, cassettiera, archivio, …) i dati cartacei ad esso affidati, affinché gli stessi non possano essere visti da terzi non autorizzati (es. addetti alle pulizie) o da terzi (visitatori) presenti nel Comune.

A fine giornata deve essere previsto il riordino della scrivania e la corretta archiviazione di tutte le pratiche d'ufficio, in modo da lasciare la scrivania completamente sgombra.

Ove possibile, si invita ad evitare la stampa di documenti digitali, anche ai fini di ridurre l'inquinamento e il consumo delle risorse in ottica ecologica.

Ove possibile, si invita ad effettuare la scansione dei documenti cartacei ed archiviarli digitalmente.

È necessario rimuovere immediatamente ogni foglio stampato da una stampante o da un'apparecchiatura fax per evitare che siano prelevati o visionati da soggetti non autorizzati.

Ove possibile, è buona norma eliminare i documenti cartacei attraverso apparecchiature trita documenti.

11. SEZIONE XI -APPLICAZIONE E CONTROLLO

a. Il controllo

Il Comune, in qualità di Titolare degli strumenti informatici, dei dati ivi contenuti e/o trattati, si riserva la facoltà di effettuare i controlli che ritiene opportuni per le seguenti finalità:

1. Tutelare la sicurezza e preservare l'integrità degli strumenti informatici e dei dati.
2. Evitare la commissione di illeciti o per esigenze di carattere difensivo anche preventivo.
3. Verificare la funzionalità del sistema e degli strumenti informatici.

Le attività di controllo potranno avvenire anche con audit e vulnerability assessment del sistema informatico. Per tali controlli il Comune si riserva di avvalersi di soggetti esterni.
Si precisa, in ogni caso, che il Comune non adotta "apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori" (ex art. 4, primo comma, l. n. 300/1970), tra cui sono certamente comprese le strumentazioni hardware e software mirate al controllo dell'utente.

b. Modalità di verifica

In applicazione del GDPR, il Comune promuove ogni opportuna misura, organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri e, comunque, a "minimizzare" l'uso di dati riferibili ai Soggetti autorizzati e allo scopo ha adottato ogni possibile strumento tecnico, organizzativo e fisico, volto a prevenire trattamenti illeciti sui dati trattati con strumenti informatici.

Il Comune informa di non adottare sistemi che determinano interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata.

In particolare eventuali sistemi atti a monitorare eventuali violazioni di legge o comportamenti anomali da parte dei Soggetti autorizzati avvengono nel rispetto del principio di pertinenza e non eccedenza, con esclusione di registrazioni o verifiche con modalità sistematiche. Al contrario possono esserci verifiche programmate ai sensi del principio di Accountability ex art. 5.2 del GDPR.

Qualora nell'ambito di tali verifiche si dovesse rilevare un evento dannoso, una situazione di pericolo o qualche altra modalità non conforme all'attività lavorativa (es. scarico di files pirata, navigazioni da cui sia derivato il download di virus informatici, ecc.) si effettuerà un avvertimento in modo generalizzato con l'invito ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

c. Modalità di Conservazione

I sistemi software sono stati programmati e configurati in modo che il soggetto autorizzato possa periodicamente cancellare i dati personali relativi agli accessi ad Internet e al traffico telematico (cronologia), la cui conservazione non sia necessaria.

Un eventuale prolungamento dei tempi di conservazione viene valutato come eccezionale e deve aver luogo solo in relazione:

1. ad esigenze tecniche o di sicurezza del tutto particolari;
2. all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
3. all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

In questi casi, il trattamento dei dati personali è limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed essere effettuato con logiche e forme strettamente correlate agli obblighi, compiti e finalità già esplicitati.

12. SEZIONE XII – SOGGETTI PREPOSTI DEL TRATTAMENTO, SOGGETTI AUTORIZZATI E RESPONSABILI

a. Individuazione dei Soggetti autorizzati

Il Comune ha individuato specifiche figure cui impartire precise istruzioni sul tipo di controlli ammessi e sulle relative modalità di trattamento del dato personale.

Per quanto riguarda i soggetti preposti al connesso trattamento dei dati (in particolare, i soggetti autorizzati della manutenzione) questi sono soggetti autorizzati di svolgere solo operazioni strettamente necessarie al perseguimento delle finalità di sicurezza informatica, senza realizzare attività di controllo a distanza, neanche di propria iniziativa.

I soggetti che operano quali amministratori di sistema o le figure analoghe cui siano rimesse operazioni connesse al regolare funzionamento dei sistemi, svolgono un'attività formativa sui profili tecnico-gestionali e di sicurezza delle reti, sui principi di protezione dei dati personali e sul segreto nelle comunicazioni.

13. SEZIONE XIII – PROVVEDIMENTI DISCIPLINARI

a. Conseguenze delle infrazioni disciplinari

Le infrazioni disciplinari alle norme del presente Disciplinare potranno essere punite, a seconda della gravità delle mancanze, in conformità alle disposizioni di legge e/o del Contratto Collettivo Nazionale del Lavoro applicato sia per il personale che per la Dirigenza, tra cui:

1. il biasimo inflitto verbalmente;
2. lettera di richiamo inflitto per iscritto;
3. multa;
4. la sospensione dalla retribuzione e dal servizio;
5. il licenziamento disciplinare e con le altre conseguenze di ragioni e di legge;

14. SEZIONE XIV – VALIDITA', AGGIORNAMENTO ED AFFISSIONE

a. Validità

Il presente Disciplinare ha validità a partire dalla data di sottoscrizione da parte del Titolare sotto riportata.

b. Aggiornamento

Il presente Disciplinare sarà oggetto di aggiornamento ogni volta che se ne ravvisi la necessità, in caso di variazioni tecniche dei sistemi del Comune o in caso di mutazioni legislative.
Ogni variazione del presente Disciplinare sarà comunicata agli soggetti autorizzati.

c. Diffusione

Il presente Disciplinare verrà pubblicato nella Intranet comunale/portale risorse umane, sul sito web istituzionale e inviato a tutti I dirigenti e dipendenti per la maggior diffusione ed ai sensi del CCNL.

Marino, li

IL TITOLARE DEI DEVICE E STRUMENTI INFORMATICI
COMUNE DI MARINO

_____