COMUNE DI FORTE DEI MARMI

Provincia di Lucca

REGOLAMENTO PER IL CORRETTO UTILIZZO DEGLI STRUMENTI INFORMATICI E TELEMATICI E DEL SISTEMA DI TELEFONIA.

Approvato con Deliberazione di C.C. n. 61 del 19.12.2018

SOMMARIO

Art. 1

Oggetto

1. Il sistema informatico ed informativo del Comune di Forte dei Marmi si basa su una rete locale estesa alle sedi comunali (P.zza Dante, Via Mazzini (2), Via Spinetti, Via Giglioli, Piazza Marconi e Via Provinciale) in cui sono dislocati gli Uffici del Comune collegate mediante una rete INTRANET.

2. Tutti i personal computer utilizzati dal personale dipendente sono collegati sulla rete locale (LAN) e dispongono di collegamento ad internet e dei servizi di posta elettronica mediante account personali e di ufficio su dominio del comune (indirizzo@comune.fortedeimarmi.lu.it). L'accesso a internet avviene tramite un unico punto di raccordo che collega all'internet service provider (ISP) che fornisce la connettività con la rete nazionale ed internazionale.

3. Ogni utente riceve uno username per fare login al dominio. Questo username è costituito dal cognome e l'iniziale del nome (es. Mario Rossi: mrossi). La gestione del dominio dell'Ente prevede l'introduzione dei profili comuni (Roaming Profiles). Questa gestione consente di replicare il profilo locale dell'utente su di un percorso di rete. In questo profilo sono contenuti sia i dati di ogni utente (la cartella documenti e lo stesso desktop), le cartelle condivise dell'ufficio, e le impostazioni dell'ambiente di lavoro (sia per il desktop che per i programmi). Questa politica di gestione consente di effettuare il backup quotidiano dei profili degli utenti ma anche di velocizzare il ripristino di una postazione di lavoro. Il profilo deve contenere soltanto i documenti e le informazioni strettamente necessarie all'attività lavorativa eliminando i file obsoleti o inutili. Questa accortezza è fondamentale in vista soprattutto dei Roaming Profiles descritti in precedenza: più un profilo è "pesante" e maggiore è il tempo necessario per effettuare connessioni e disconnessioni dell'utente sulla postazione di lavoro.

4. Il presente regolamento disciplina le modalità di accesso e di uso della rete informatica e telematica oltre che del sistema di telefonia del Comune di Forte dei Marmi e dei servizi che, tramite la rete stessa, è possibile ricevere o offrire.

Art. 2

Principi generali - diritti e responsabilità

1. Il Comune di Forte dei Marmi promuove la diffusione della cultura della sicurezza informatica, tema di particolare importanza soprattutto in relazione alla grande quantità di informazioni su cittadini e imprese che viene trattata dalle Pubbliche Amministrazioni e alla gravità dei danni causati da episodi di pirateria informatica. L'uso delle apparecchiature informatiche da parte dei dipendenti deve quindi essere disciplinato da Norme certe poiché da comportamenti non leciti, anche inconsapevoli, possono derivare gravi conseguenze sia sul piano tecnico (es. perdita di dati) che su quello penale, oltre a problemi di immagine all'Ente stesso. Inoltre una corretta applicazione del "Codice in Materia di Protezione dei Dati Personali" D.lgs. 30 giugno 2003 n. 196, modificato con D.lgs. 10 agosto 2018 n. 101 (in accordo al nuovo Regolamento UE 679/2016), comporta in via prioritaria la definizione di regole circa l'utilizzo delle tecnologie quando queste sono utilizzate per il trattamento di dati personali comuni o sensibili. L''utilizzo delle risorse informatiche e telematiche Aziendali deve quindi sempre ispirarsi al principio della diligenza e correttezza. Il Comune di Forte dei Marmi intende pertanto adottare l'elenco di norme contenute in questo regolamento per contribuire alla massima diffusione della "Cultura della sicurezza" ed evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati.

2. L'utilizzo degli strumenti informatici, della Rete Informatica e Telematica del Comune di Forte dei Marmi (internet, posta elettronica e del Sistema di Telefonia quali strumenti utili a perseguire

con efficacia ed efficienza le proprie finalità istituzionali) si deve ispirare al rispetto dei principi e delle linee guida delineati dalla normativa vigente. Gli utenti devono agire nel rispetto dell'integrità dei sistemi e delle relative risorse fisiche consapevoli delle potenzialità offerte dagli strumenti informatici e telematici e si impegnano ad agire con responsabilità e a non commettere abusi aderendo a un principio di autodisciplina.

3. Le dotazioni informatiche e telefoniche (p.c.,notebook, tablet, smartphone,ecc.) affidate al dipendente sono uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa non è consentito in quanto può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

4. Il CED - Informatizzazione provvede a dotare tutti i personal computer assegnati agli utenti con sistema operativo e sue estensioni: antivirus, programmi di office automation (programmi per la redazione di documenti, di fogli elettronici, di gestori di database), rispettando le normative sugli open source che prevedono l'utilizzo dei programmi gratuiti presenti in rete per permettere un notevole risparmio economico. Tali Personal computer sono connessi alla rete locale e sono dotati, a seconda della loro collocazione all'interno della struttura organizzativa dell'ente, dei programmi dedicati alle gestioni specifiche cui l'Ufficio è preposto (contabilità finanziaria, Gestione economica e giuridica del personale, atti amministrativi, lavori pubblici, ecc.). Il CED - Informatizzazione provvede a mantenere la corretta configurazione dei personal computers e ad impedire la modifica della stessa utilizzando le tecniche e gli strumenti opportuni (creazione di utenti di dominio con autorizzazioni limitate, impostazione password del BIOS, ecc).

5. II Personal Computer affidato al dipendente è uno strumento di lavoro e ognuno è responsabile dell'utilizzo delle dotazioni informatiche ricevute in assegnazione nell'ambito del servizio assegnato e per le competenze che deve gestire. Ogni Dirigente deve segnalare tempestivamente al CED - Informatizzazione ogni cambiamento relativo ai dipendenti assegnati (assunzioni, spostamenti, cambio di mansioni e/o profilo, ecc.), anche per consentire/eliminare permessi di accesso/modifica a email dell'ufficio e a cartelle/files condivisi. Il Dirigente è l'unico che può chiedere al CED – Informatizzazione l'attivazione/disattivazione delle caselle email o la loro cancellazione/interruzione.

6. Il Personal Computer deve essere spento alla fine della giornata lavorativa fatto salvo i casi in cui, dietro comunicazione degli addetti del CED - Informatizzazione, vada lasciato acceso per eseguire attività di manutenzione, (antivirus, deframmentazioni dell'Hard Disk etc).

7. In caso di assenze prolungate dall'ufficio (pausa pranzo) o ogni qualvolta l'utente ritenga di non essere in grado di presidiare l'accesso alla propria stazione di lavoro, è opportuno effettuare una disconnessione dell'utente o bloccare la postazione in modo che per la sua riattivazione sia necessario inserire di nuovo la propria password. L'utilizzo da parte di terzi non può essere provato qualora una postazione di lavoro connessa alla rete sia lasciata incustodita.

8. Le unità 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. Su queste unità, vengono svolte regolari attività di controllo con conseguente cancellazione dei files non pertinenti all'attività lavorativa. Il CED - Informatizzazione può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosa per la sicurezza, da qualsiasi dotazione informatica.

9. Costituisce buona regola la periodica (mensile) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. E' infatti assolutamente da evitare un'archiviazione ridondante.

10. Tutti i supporti magnetici e rimovibili riutilizzabili (dischi, chiavette Usb, memory card, ecc.) contenenti dati personali devono essere trattati con particolare cautela, onde evitare che il loro

contenuto possa essere recuperato. I supporti removibili contenenti dati sensibili devono essere custoditi in armadi/cassetti chiusi a chiave.

Art. 3

Utilizzo di dotazioni informatiche portatili

1. L'utente è responsabile delle dotazioni informatiche portatili, quali notebook, tablet, smartphone, ecc., assegnategli e deve custodirle con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

2. Alle dotazioni informatiche portatili si applicano le regole di utilizzo previste per i normali Pc connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.

Art. 4

Utilizzo di fotocopiatrici e stampanti di rete

1. E' cura del personale effettuare la stampa dei dati solo se strettamente necessaria e, nel caso avvenga su stampanti di rete ubicate in luoghi facilmente accessibili al pubblico, deve essere presidiata. E' buona regola evitare di stampare documenti o file pesanti o non supportati su stampanti comuni. In caso di necessità la stampa in corso può essere cancellata.

2. Il cambio cartucce va fatto senza causare danni all'apparecchiatura: se non si è sicuri di come procedere alla sostituzione, contattare gli addetti al sistema informatico.

3. Nel caso si debbano cambiare, per particolari esigenze, le impostazioni di un fotocopiatore e/o stampante, contattare gli addetti al sistema informatico.

Art. 5

Abusi e attività vietate

1. Si intende con abuso qualsiasi violazione del presente regolamento e di altre norme civili, penali e amministrative che disciplinano le attività e i servizi svolti sulla rete e di condotta personale;

2. E' vietato ogni tipo di abuso. In particolare è vietato:

• Usare la rete in modo difforme da quanto previsto dal presente regolamento;

• Usare la rete in modo difforme da quanto previsto dalle leggi penali, civili e amministrative;

• Utilizzare la rete aziendale e internet per scopi incompatibili con l'attività istituzionale del Comune di Forte dei Marmi;

• Utilizzare codici di accesso non propri;

• Cedere a terzi i propri codici di accesso al sistema;

• Conseguire l'accesso non autorizzato a risorse di rete interne o esterne;

• Agire con attività che influenzino negativamente la regolare operatività della rete e ne restringano l'utilizzabilità e le prestazioni per altri utenti; • Fare o permettere ad altri trasferimenti non autorizzati di informazioni (software, basi dati, documenti, ecc.)

• Installare, eseguire o diffondere su qualunque dotazione informatica e sulla rete, programmi destinati a danneggiare o sovraccaricare i sistemi o la rete (virus, cavalli di troia, worms, spamming della posta elettronica, programmi di file sharing);

• Installare o eseguire programmi software non autorizzati e non compatibili con le attività istituzionali;

• Cancellare, disinstallare o copiare programmi software per scopi personali; • Installare componenti hardware non compatibili con le attività istituzionali

• Rimuovere, danneggiare o asportare componenti hardware;

• Utilizzare la posta elettronica inviando e ricevendo materiale che violi le leggi;

• Leggere, copiare o cancellare files e software di altri utenti, senza averne l'autorizzazione esplicita;

• Abbandonare il posto di lavoro lasciandolo collegato alla rete.

3. E' vietato adottare comportamenti illeciti in ordine all'utilizzazione di supporti vergini, memorie e apparecchi di registrazione (riproduzione di fonogrammi e videogrammi per uso personale, cessione di tali prodotti, ecc.)

Art. 6 –

Attività consentite all'Amministratore di sistema

1. Nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori, è consentito all'Amministratore di sistema:

• Monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare il corretto utilizzo delle risorse di rete (sia intranet che internet), delle dotazioni informatiche e degli applicativi;

• Rimuovere programmi software e componenti hardware.

2. L'Amministratore di sistema, su richiesta del Dirigente di competenza, può accedere alla casella di posta elettronica del personale non più in servizio e/o degli amministratori non più in carica, per salvare eventuali mail di interesse per l'ente, prima di disattivare definitivamente la casella stessa. Sarà cura degli interessati eliminare eventuali mail o farne copia di backup, prima della cessazione del rapporto di lavoro o del mandato.

Art. 7

Soggetti che possono avere accesso alla rete

Dopo le necessarie autorizzazioni fornite dai Dirigenti responsabili:

1. Hanno la possibilità di accedere al sistema informatico del Comune di Forte dei Marmi i dipendenti, le ditte fornitrici di software per motivi di manutenzione limitatamente alle applicazioni di loro competenza, i collaboratori a qualsiasi titolo impegnati nelle attività istituzionali limitatamente al periodo di collaborazione se autorizzati dal Dirigente di competenza.

2. Per fini istituzionali hanno la possibilità di accedere al sistema informatico il Sindaco, nonché gli Assessori e gli altri amministratori nell'ambito delle loro competenze.

3. L'Amministratore di sistema può regolamentare l'accesso alla rete di determinate categorie di utenti, quando questo è richiesto per ragioni tecniche e/o dal Dirigente di competenza.

4. L'accesso agli applicativi è consentito agli utenti che, per motivi di servizio, ne devono fare uso: quando un dipendente viene trasferito, il Dirigente dovrà richiedere la rimozione dei privilegi di accesso e eventualmente concederli ad altri dipendenti.

Art. 8

Modalità di accesso alla rete e agli applicativi

1. L'utente che ottiene l'accesso alla rete e agli applicativi è tenuto ad osservare il presente regolamento e le altre norme disciplinanti le attività e i servizi che si svolgono via rete ed è tenuto a non commettere abusi e a non violare i diritti degli altri utenti e dei terzi.

2. L'utente che ottiene l'accesso alla rete e agli applicativi si assume la totale responsabilità delle attività svolte tramite la rete.

3. Qualsiasi accesso alla rete e agli applicativi viene associato ad una persona fisica cui imputare le attività svolte utilizzando il codice utente.

4. Al primo collegamento alla rete e agli applicativi, l'utente deve modificare la password (parola chiave) comunicatagli dall'Amministratore di Sistema e deve rispettare le seguenti norme:

Password di accesso

a) al dominio

Al momento della consegna di una nuova postazione di lavoro ad un dipendente comunale il CED - Informatizzazione provvede ad assegnargli una username (formata dal proprio cognome e l'iniziale del nome) ed una password provvisoria per effettuare il primo accesso al dominio e a tutti i servizi che offre (stampanti di rete, condivisioni,…).

Tale password deve essere cambiata dall'utente al primo accesso al PC. La password che l'utente assegna deve soddisfare alcuni criteri di complessità quali:

• Lunghezza: minimo 8 caratteri appartenenti a tre delle 4 categorie seguenti:

• Lettere maiuscole (A-Z)

• Lettere minuscole (a-z)

• Cifre da 0 a 9

• Caratteri non alfanumerici (ad es. ,!,$,#,%)

• Non deve contenere una parte o tutto il nome di account dell'utente

• Non devono inoltre essere utilizzati evidenti riferimenti alla propria persona (non usare il nome dei figli, del marito o altri attributi facilmente riconducibili alla persona in questione) o alla struttura di appartenenza.

Il sistema è impostato in modo da "ricordare" le 24 password utilizzate in precedenza e quindi riconosce e rifiuta, una password troppo simile alle precedenti. Tale password deve rimanere segreta e non deve essere rivelata ad altre persone. La password dovrà essere custodita con modalità idonea a garantire la sua sicurezza (no ai post-it affissi ai monitor, tastiere, telefoni…). Mantenere segreta la propria password tutela l'utente nei confronti di usi indebiti delle proprie credenziali di accesso. In caso di necessità di accesso alla postazione e il dipendente non sia presente, il dirigente del settore cui il dipendente afferisce può chiedere agli amministratori di dominio di resettare la password del dipendente assegnandone una provvisoria. Tale password dovrà essere cambiata al momento del rientro in servizio del dipendente. Ogni utente può, a sua discrezione, cambiare in ogni momento la propria password. Nel caso in cui tale cambiamento non avvenga in modo spontaneo, il gestore del dominio obbliga al cambio password ogni 3/6 mesi a seconda dei dati gestiti dall'utente.

b) Password di accesso alle procedure

All'utente vengono assegnate password per l'accesso ad ogni procedura software che utilizza. Anche queste dovranno ugualmente essere mantenute strettamente riservate.

5. La gestione del dominio prevede l'introduzione dei profili comuni (Roaming Profiles). Gli utenti devono salvare i propri dati esclusivamente all'interno del proprio profilo del sistema locale, perché è questo percorso che viene salvato quotidianamente sul file server e su nastro magnetico. Qualora per esigenze diverse questo non fosse possibile, gli utenti dovranno segnalare il problema al CED - Informatizzazione per gestire il backup dei dati collocati in posizioni diverse dalla cartella contenente il profilo.

Art. 9

Internet: la navigazione web

1. L'accesso ad Internet è abilitato su tutti i personal computers connessi alla rete locale. Il PC abilitato alla navigazione in internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. Non è quindi consentito l'utilizzo della connessione:

• per scopi personali

• per il collegamento a siti ed il trasferimento di files il cui contenuto non sia in relazione con l'attività lavorativa del dipendente • per la visione di filmati, l'ascolto di files audio, l'utilizzo di programmi di chat e messaggistica il cui contenuto non sia in relazione con l'attività lavorativa del dipendente.

Sono espressamente vietate le connessioni ad Internet su linea telefonica, con modem ed abbonamenti personali.

2. La razionalizzare delle risorse INTERNET, anche in termini di banda, è garantita da un proxy server che permette il monitoraggio del traffico internet in uscita. Tale strumento consente di rilevare, per ogni postazione, l'indirizzo di destinazione raggiunto unitamente alla dimensione ed al tipo di file eventualmente scaricato. Consente inoltre di adottare misure di filtraggio sulle connessioni, bloccando autonomamente i contenuti malevoli e/o incompatibili con le policies aziendali sull'utilizzo del servizio, evidenziando i problemi e le anomalie relativi al traffico di rete. A tal proposito vengono individuati e censiti categorie di siti considerati correlati o meno con la prestazione lavorativa. I siti considerati incoerenti sono inseriti in una black list. Tale black list è continuamente aggiornata sulla base di analisi effettuate periodicamente su dati aggregati delle navigazioni effettuate dalle postazioni connesse alla LAN aziendale.

3. Qualora, tali sistemi di filtraggio impediscano l'utilizzo di siti o risorse utili all'attività lavorativa, il dipendente interessato deve inviare segnalazione scritta al CED - Informatizzazione.

4. Il Comune di Forte dei Marmi può configurare sistemi o utilizzare filtri che prevengano determinate operazioni, reputate incoerenti con l'attività lavorativa, quali l'upload e/o il download di file o software aventi particolari caratteristiche (dimensionali o di tipologia);

5. Non è consentito il download di software o di file multimediali che non sia previamente autorizzato dai Responsabili di Area/Servizio, in accordo con l'amministratore di sistema.

6. I dati registrati nei log relativi alla navigazione internet dalle dotazioni informatiche collegate alla rete comunale sono:

• Indirizzo IP dello strumento che si collega ad internet;

• Indirizzo internet del server a cui ci si collega;

• Data e ora di inizio collegamento;

• Indirizzo internet completo a cui ci si collega (URL);

• Porta dello strumento di collegamento;

• Traffico effettuato

I contenuti delle pagine visualizzate non sono memorizzati.

Art. 10

Posta elettronica

1. La posta elettronica è forse il veicolo per eccellenza per la diffusione di infezioni virali; a tal scopo è in funzione un sistema antivirus centralizzato che verifica automaticamente la disponibilità degli aggiornamenti e provvede alla loro installazione. Tale sistema monitorizza anche gli allegati di posta elettronica.

2. L'indirizzo di posta elettronica con dominio @comune.fortedeimarmi.lu.it è strumento di lavoro ed un bene messo a disposizione dell'utente per soli fini lavorativi. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

3. Ogni utente viene dotato di un account personale mentre dirigenti o loro delegati hanno accesso anche ad un account di ufficio/servizio.

4. La casella di posta deve essere mantenuta in ordine, cancellando i messaggi inutili e soprattutto gli allegati ingombranti. Nel caso di mittenti sconosciuti o messaggi insoliti, per non correre il rischio di essere infettati da virus, occorrerà cancellare i messaggi senza aprirli. Anche nel caso in cui i messaggi provengano da mittenti conosciuti ma che contengano collegamenti o allegati sospetti (file con estensione .exe, .scr, .pif, .bat, .cmd) non devono essere aperti. E' buona norma utilizzare, nel caso di invio di allegati pesanti, i formati compressi (*.zip, *.rar o *.jpg).

5. Messaggi di posta elettronica di provenienza non nota o palesemente provenienti da "spamming" devono essere immediatamente cancellati senza essere prima aperti.

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

7. E' buona norma limitare lo scambio di dati personali attraverso la posta elettronica. Qualora ciò si rendesse necessario, dovranno essere osservate le seguenti cautele:

• Verificare l'indirizzo di posta elettronica del destinatario;

• Non inserire i dati nel testo del messaggio;

• Inviare i dati come allegato al messaggio di posta elettronica. L'allegato dovrà essere protetto con modalità idonee ad impedire l'illecita o fortuita acquisizione delle informazioni trasmesse da parte di soggetti diversi da quello cui sono destinati (es. password per l'apertura del file da rendere nota agli interessati tramite canali di comunicazione differenti da quelli utilizzati per la spedizione dell'allegato).

8. Nello scambio di comunicazioni istituzionali va data priorità all'utilizzo della posta elettronica certificata.

9. Per lo scambio di documenti fra uffici diversi non si deve utilizzare la posta elettronica ma le condivisioni create in rete per ogni singolo ufficio. Qualora la condivisione di documenti debba avvenire tra uffici diversi, si possono usare le aree di interscambio chiedendo al CED - Informatizzazione di impostare dei diritti ad hoc in modo da tutelare questo scambio di documenti.

Art. 11

Controlli

1. Nell'effettuare controlli sull'uso degli strumenti elettronici il Comune di Forte dei Marmi evita un'interferenza ingiustificata sui diritti dei lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata.

2. L'eventuale controllo è lecito solo se sono rispettati i principi di pertinenza e non eccedenza.

3. Il datore di lavoro può adottare eventuali misure che consentano la verifica di comportamenti anomali. Sarà preferito un controllo preliminare su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree. Il controllo si concluderà con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. L'avviso potrà essere circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia. In assenza di successive anomalie non è di regola giustificato effettuare controlli su base individuale.

4. Non sono consentiti controlli prolungati, costanti o indiscriminati.

Art. 12

Conservazione

1. I sistemi software sono programmati e configurati in modo da cancellare periodicamente ed automaticamente i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.

2. In assenza di particolari esigenze tecniche o di sicurezza, la conservazione temporanea dei dati relativi all'uso degli strumenti elettronici deve essere giustificata da una finalità specifica e comprovata e limitata al tempo necessario e comunque nel rispetto delle indicazioni del Garante per la privacy, (vedasi apposito regolamento).

3. L'eventuale ed eccezionale prolungamento dei tempi di conservazione potrà aver luogo solo in relazione:

• Ad esigenze tecniche o di sicurezza del tutto particolari;

• All'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;

• All'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria o norma di legge.

In questi casi, il trattamento dei dati personali/sensibili, tenendo conto delle prescrizioni contenute nelle autorizzazioni generali adottate dal Garante, dovrà essere limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed essere effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità già esplicitati.

4. I dati integrali della navigazione internet sono conservati nei server del Comune di Forte dei Marmi. I dati vengono conservati per almeno due anni salvo diverso limite imposto da norme di legge, o necessario per l'attuazione di provvedimenti disciplinari. Tali dati sono accessibili agli addetti del sistema informatico. L'accesso ai dati dei log è fatto in forma graduale, in modo da considerarli in prima analisi in forma complessiva ed anonima, cioè non direttamente riconducibili ad un utente.

Art. 13

Telefonia fissa e mobile

1. Gli strumenti di telefonia (sia fissa che mobile) messi a disposizione dal Comune costituiscono strumento di lavoro e ne è consentito l'utilizzo unicamente per finalità attinenti o comunque connesse all'esercizio dell'attività lavorativa.

2. E' escluso l'uso per scopi privati e/o personali, salvo che tale uso sia motivato da ragioni di urgenza e di necessità. E' in ogni caso vietato l'uso reiterato e prolungato per fini personali.

3. L'utilizzo di apparecchiature di telefonia mobile è finalizzato a garantire il miglioramento delle comunicazioni per necessità di servizio e la realizzazione di un'economia di spesa mediante la riduzione dell'uso della tecnologia fisso-mobile. A tal fine gli utilizzatori dei telefoni cellulari hanno l'obbligo di mantenere in funzione il telefono cellulare durante le ore di servizio, durante le ore di reperibilità, ove previste, ed in tutti i casi in cui le circostanze concrete lo rendano opportuno.

4. Ogni assegnatario di apparecchio cellulare è responsabile dell'uso appropriato e della diligente conservazione dell'apparecchio, che non può essere ceduto a colleghi o terzi a nessun titolo. Tutti i telefoni cellulari devono essere utilizzati da parte degli assegnatari, in modo strettamente pertinente alla propria attività lavorativa o carica istituzionale e per un utilizzo appropriato, efficiente, corretto e razionale. Nella definizione di attività lavorativa devono essere ricomprese anche le attività che siano strumentali e connesse alla stessa quali, ad esempio, i rapporti con le istituzioni, le aziende che gestiscono servizi e le associazioni del territorio.

5. È consentito l'utilizzo dei telefoni cellulari di servizio per chiamate personali o comunque diverse da quelle di servizio esclusivamente nel caso in cui sia stata attivata apposita opzione che consente di addebitare o quantomeno di rendicontare i relativi costi direttamente all'utilizzatore. In questo caso, l'utilizzatore dovrà obbligatoriamente effettuare le chiamate antecedendo al numero telefonico il prefisso indicato dalla compagnia telefonica per consentire l'addebito separato dei relativi costi.

6. Su richiesta di alcuni intestatari di cellulari aziendali sono stati attivati dei meccanismi di autoregolazione della spesa relativa al traffico telefonico effettuato con il cellulare in dotazione che, al raggiungimento di una soglia mensile, viene addebitato sugli stipendi dei richiedenti

Art. 14

Controlli uso telefonia

1. L'Ente effettua controlli sul corretto utilizzo l'utilizzo degli apparecchi di telefonia fissi/mobili messi a disposizione al fine di verificarne il corretto utilizzo e monitorare e ridurre la relativa spesa.

2. I controlli effettuati dall'Ente devono rispettare i principi di necessità, proporzionalità, imparzialità, trasparenza e protezione dei dati personali. Nel caso in cui vengano riscontrate evidenti anomalie o rilevanti scostamenti nel volume complessivo di traffico relativo alla singola utenza rispetto alla media registrata nei sei mesi precedenti ovvero alla media registrata da altri utilizzatori, l'Ente disporrà un controllo più puntuale su tale traffico telefonico congiuntamente all'assegnatario del cellulare e adotterà le opportune misure per l'eliminazione dell'anomalia.

3. Nel valutare i risultati del controllo si dovranno tenere in considerazione eventuali necessità, anche temporalmente limitate, connesse a particolari finalità istituzionali o di servizio, a conoscenza del Responsabile del Servizio interessato.

Art. 15

Pubblicazioni, attivazioni e manutenzione procedure

1. Per quanto riguarda le pubblicazioni sul sito internet istituzionale www.comune.fortedeimarmi.lu.it – www.comunefdm.it , il CED – Informatizzazione garantisce l'utilizzo dei suddetti Domini, fornisce assistenza e pubblica seguendo le indicazioni fornite dagli uffici/servizi all'email: pubblicazionesito@comunefdm.it .

Allo scopo di uniformare le modalità di pubblicazione di informazioni varie sul sito web, si forniscono le seguenti indicazioni generali per ottimizzare lo sfruttamento delle potenzialità delle pagine web migliorandone nel contempo l'accessibilità da parte degli utenti.

A) Pubblicazioni generiche notizie da inserire in home page

Ogni ufficio è tenuto a prendere contatto con l'Ufficio Stampa che è l'organo ufficiale del nostro Comune per la redazione di ogni comunicazione rivolta all'esterno, l'ufficio stampa valuta se è il caso di pubblicare in prima pagina e invia il comunicato al CED-Informatizzazione per la messa online.

B) Pubblicazioni di generiche notizie da inserire in home page con inserimento di modulistica varia

Oltre al contatto con l'Ufficio Stampa, come sopra, investire l'Ufficio CED-Informatizzazione per l'inserimento di eventuale modulistica (specificando che andrà inserita nell'articolo dell'ufficio Stampa e/o in altre pagine, per esempio modulistica Ufficio ambiente).

C) In Home Page, sopra *Ultime Notizie – Concorsi comunali* è possibile inserire una notizia fissa di importanza rilevante.

D) Pubblicazioni Bandi di gara

Format generale da seguire al momento dell' invio dei documenti:

1. Nome del bando e dei relativi files

(visto che i files e le diciture verranno inserite facendo copia-incolla, e verranno visualizzati sul web come inviato dai proponenti, si chiede attenzione all'ortografia e non scrivere tutto maiuscolo che sul web è sinonimo di URLARE).

2. Durata/Scadenza del Bando

Se richiesto sarà inserita, sotto il titolo la dicitura per es.: "Il Bando scade il 28 febbraio alle ore 12:30"

3. Ulteriori informazioni

Andranno concordate con CED-Informatizzazione per eventuale fattibilità.

4. Ulteriori aggiornamenti

L'inserimento dell'eventuale esito di gara/procedura andrà richiesto dall'ufficio proponente tramite apposita email che ricordi esattamente il titolo della procedura/gara.

L'eventuale rimozione/spostamento del bando intero in altre categorie (archiviate, scadute etc) andrà richiesto sempre tramite email il giorno della rimozione e non con giorni di anticipo.

E) Pubblicazione della modulistica, dei bandi e di modulistica varia:

L'Ufficio CED-Informatizzazione non si assume la competenza di rinominare sul sito i file ricevuti. Nel caso dell'inserimento di files all'interno di una cartella già esistente, andrà specificato dove effettuare la pubblicazione e/o la sostituzione.

F) Non è possibile pubblicare file di dimensioni superiori a 20 mb, e foto più grandi di 800x800 pixel.

G) Sarà compito dell'ufficio che richiede la pubblicazione:

- Il controllo delle pubblicazioni effettuate dal CED-Informatizzazione e la comunicazione di eventuali errori.
- La comunicazione al CED-Informatizzazione della rimozione del Bando pubblicato o lo spostamento dello stesso in altre cartelle del sito comunale (Bandi scaduti, Bandi archiviati, etc).

H) Sarà compito del CED-Informatizzazione:

- La pubblicazione delle varie richieste entro le ore 14 o entro il giorno seguente se necessitano di lunga lavorazione o se pervenute dopo le ore 13:30. (Farà testo l'orario di invio ricezione avvenuta lettura)
- La comunicazione all'ufficio proponente dell'avvenuta pubblicazione o dei problemi eventualmente presentatisi.
- Essere a disposizione dei vari uffici per la pubblicazione presso l'ufficio CED in affiancamento a incaricati dal Dirigente/ Resp. P.O. di competenza per lavori complessi.
- Favorire i colleghi che volessero effettuare corsi presso la ditta che gestisce il Sito, se autorizzati dal Dirigente di competenza.

I) Eventuali richieste di modifiche della struttura del sito, dovranno essere autorizzate dal Dirigente/CED-Informatizzazione.

2. Nel caso di altro tipo di pubblicazioni, (amministrazione trasparente, trasparenza amministrativa, Albo pretorio etc.) i singoli servizi/uffici dovranno ottemperare in maniera autonoma a quanto la Legge del caso chiede di adempiere.

3. Per l'iscrizione ad eventuali servizi esterni (per es. Il portale dell'automobilista, marche temporali, siti per procedure DURC, antimafia, massive etc.). Il Ced – Informatizzazione fornisce un aiuto al momento dell'attivazione per eventuali upgrade del pc comunale, gli uffici devono provvedere in maniera autonoma alle attivazioni, richieste password e soluzione dei malfunzionamenti se non dovuto a problematiche interne, rivolgendosi al servizio tecnico della procedura stessa.

4. In caso di attacco virus, Il Ced – Informatizzazione fornisce i dettagli utili per la pulizia del computer e gli utenti devono attenersi a dette procedure in maniera scrupolosa.

Art. 16

Sanzioni

In caso di abuso, a seconda della gravità del medesimo, e fatte salve ulteriori conseguenze di natura penale, civile e amministrativa, possono essere comminate le sanzioni disciplinari previste dalla normativa vigente in materia e dal codice disciplinare.

Art. 17

Informativa

Il contenuto del presente regolamento integra l'informativa ai dipendenti e ai collaboratori ai sensi dell'art.13 del D.Lgs. 196/2003 (Codice della privacy), modificato con D.lgs. 10 agosto 2018 n. 101 e in accordo al nuovo Regolamento UE 679/2016.

Art. 18

Norma finale

Il presente regolamento abroga ogni provvedimento precedente che disciplina la materia.