COMUNE DI FONDI
(Provincia di Latina)

ORIGINALE

Deliberazione n. 2
del 8/1/2013

VERBALE DI DELIBERAZIONE DEL CONSIGLIO COMUNALE
Adunanza straordinaria di I convocazione - seduta pubblica

Oggetto: Regolamento per l'utilizzo dei Sistemi Informativi

L'anno duemilatredici, addì otto del mese di gennaio alle ore 19,30 nella sala delle adunanze consiliari

Previa l'osservanza di tutte le formalità prescritte dalla vigente legge comunale e provinciale, vennero oggi convocati a seduta i componenti del Consiglio Comunale
nelle persone dei sigg.ri:

		Presente	Assente
1) Salvatore De Meo	Sindaco	1	
2) Parisella Piero	Componente	2	
3) Trani Giovanni	Componente	3	
4) La Rocca Guido	Componente	4	
5) Sansoni Alessandro	Componente	5	
6) Carnevale Marco Antonio	Componente	6	
7) Corina Luigi	Componente	7	
8) Mattei Vincenzo	Componente	8	
9) Leone Oronzo	Componente	9	
10) Muccitelli Roberta	Componente	10	
11) Refini Vincenzo	Componente	11	
12) Paparello Elio	Componente	12	
13) Spagnardi Claudio	Componente	13	
14) Saccoccio Carlo	Componente	14	
15) Coppa Biagio	Componente	15	
16) Gentile Sergio	Componente	16	
17) Giuliano Elisabetta	Componente	17	
18) Marino Maria Luigia	Componente	18	
19) Di Manno Giulio Cesare	Componente		1
20) Cima Maurizio Vincenzo	Componente	19	
21) Cardinale Franco	Componente		2
22) Fiore Giorgio	Componente		3
23) Turchetta Egidio	Componente	20	
24) Padula Claudio	Componente	21	
25) Forte Antonio	Componente	22	
26) Paparello Maria Civita	Componente	23	
27) Faiola Arnaldo	Componente	24	
28) Fiore Bruno	Componente		4
29) Di Manno Giancarlo	Componente	25	
30) De Luca Luigi	Componente		5
31) Trani Vincenzo Rocco	Componente	26	

Assiste il segretario generale dott. Francesco Loricchio
Essendo legale il numero degli intervenuti, la prof.ssa Maria Luigia Marino assume la presidenza e dichiara aperta la seduta per la trattazione dell'argomento sopra indicato

IL CONSIGLIO COMUNALE

Premesso che:

- la diffusione delle tecnologie informatiche e telematiche ed il progressivo passaggio della società verso modelli di comunicazione sempre più integrati ed interconnessi, rende fondamentale per ogni realtà organizzativa e lavorativa, lo sviluppo di una cultura della sicurezza del proprio patrimonio informativo e della tutela dei diritti degli interessati;
- è dovere dell'Ente individuare il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione per il trattamento dei dati personali, nonché adottare idonee misure di sicurezza per assicurare la disponibilità e l'integrità di sistemi informativi, anche per prevenire utilizzi indebiti che possono essere fonte di responsabilità;

Ritenuto che l'elevato uso della tecnologia informatica (e in particolare l'accesso alla rete informatica e telematica, Internet e posta elettronica) come strumento di lavoro in questo Comune, impone la necessità di regolamentarne l'utilizzo, allo scopo di fornire agli utenti, (dipendenti, amministratori e collaboratori,) adeguata informazione circa le modalità da seguire per un corretto utilizzo degli strumenti e delle risorse informatiche e telematiche messe loro a disposizione per lo svolgimento delle proprie mansioni istituzionali, in modo che possano collaborare alla politiche di sicurezza messe in atto;

Ritenuto inoltre di porre in essere adeguati e commisurati sistemi di controllo sul corretto utilizzo degli strumenti e delle risorse informatiche e telematiche, senza che ciò possa in alcun modo invadere e violare la sfera personale del lavoratore e quindi il suo diritto alla riservatezza ed alla dignità come sancito dallo Statuto dei Lavoratori e dal D.Lgs. 196/03;

Richiamate:

- il D.lgs.30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali);
- le "Linee guida per posta elettronica e internet" adottate dal Garante con deliberazione n. 13 del 1° marzo 2007;
- la circolare n. 2/09 avente ad oggetto "Utilizzo di internet e della casella di posta istituzionale sul luogo di lavoro" con la quale il Dipartimento della Funzione Pubblica invita le Pubbliche Amministrazioni ad attuare tutte le misure di informazione, controllo e verifica consentite al fine di regolamentare la fruizione delle risorse ICT (Information e Communication Technology) e responsabilizzare i dipendenti nei confronti di eventuali utilizzi non coerenti con la prestazione lavorativa e non conformi alle norme che disciplinano il lavoro alle dipendenze delle pubbliche amministrazioni;

Visto l'allegato "Regolamento per l'utilizzo dei Sistemi Informativi" predisposto dal Settore n. 1 del Comune di Fondi", che si allega alla presente deliberazione per farne parte integrante e sostanziale;

Precisato che tale regolamento:

- si conforma alle indicazioni fornite dal Garante per la Protezione dei dati personali che con deliberazione n. 13 del 1 marzo 2007, ha emanato le linee guida in materia di utilizzo di strumenti informatici e telematici, nonché della posta elettronica e della rete Internet, nel rapporto di lavoro, oltre alla normativa in vigore;
- si configura come strumento a tutela dei diritti patrimoniali dell'Ente ed a garanzia della sicurezza ed integrità del proprio patrimonio informativo;

- si caratterizza come strumento di garanzia a favore di tutti coloro che svolgono un rapporto di lavoro o di servizio a beneficio dell'Ente, nella misura in cui costituisce una informativa preventiva, fornita a tutti questi soggetti, circa termini, casi e modalità di verifica del corretto utilizzo degli strumenti informatici e telematici messi a loro disposizione per le attività di lavoro o di servizio;

Visto il verbale n. 29 del 20 dicembre 2012 della Commissione Consiliare permanente Contabilità, Bilancio, Affari Generali, agli atti dell'ufficio competente;

Ritenuto di adottare l'allegato "Regolamento per l'utilizzo dei Sistemi Informativi" del Comune di Fondi, dando atto che lo stesso dovrà essere reso noto a tutti i dipendenti con le forme più efficaci ed immediate;

Tenuto conto della relazione del consigliere Alessandro Sansoni nonché degli interventi dei Signori Consiglierei, le cui trascrizioni allegate costituiscono parte integrate e sostanziale del presente atto;

Dato atto che al momento della votazione risulta assente il Consigliere Maria Civita Paparello;

Con la seguente votazione: Favorevoli n. 22; Astenuti n. 2 (Turchetta Egidio, Padula Claudio),

D E L I B E R A

Per i motivi di cui in premessa e che qui si intendono integralmente riportati:

1) **Di approvare** l'allegato "Regolamento per l'utilizzo dei Sistemi Informativi", che si compone di n. 17 articoli;

2) **Di individuare** nel Settore n. 1 l'unità organizzativa deputata ad emanare ed aggiornare le regole tecniche necessarie per l'attuazione delle disposizioni di carattere generale contenute nel Regolamento e a supervisionare sulla loro corretta attuazione da parte degli Uffici;

3) **Di disporre** che i Dirigenti dei Settori prestino la necessaria collaborazione affinché vengano attuate tutte le disposizioni contenute nel Regolamento citato.

COMUNE DI FONDI

(Provincia di Latina)

Regolamento per l'utilizzo dei Sistemi Informativi

Approvato con Deliberazione di Consiglio Comunale n. 2 del 08/01/2013

Negli ultimi anni l'organizzazione del lavoro è stata sottoposta ad un imponente processo di informatizzazione.

In tale contesto i servizi di rete, tra cui Posta elettronica e Internet, sono diventati strumenti quotidiani indispensabili per l'esercizio dell'attività lavorativa dal momento che consentono l'immediatezza, la democratizzazione e la trasversalità dell'informazione.

Con la Direttiva n. 2/2009, il Dipartimento della Funzione Pubblica ha riepilogato i principi e le regole cui attenersi nell'utilizzo di internet e della casella di posta elettronica sul luogo di lavoro.

Il documento richiama, per una più approfondita definizione della materia, le Linee guida adottate in merito dal Garante per la protezione dei dati personali, al fine di contemperare le esigenze di riservatezza del dipendente con quelle di esercizio del controllo da parte del datore di lavoro ai fini di un corretto utilizzo degli strumenti in questione.

Poiché le informazioni di carattere personale trattate possono riguardare, oltre all'attività lavorativa anche la sfera personale e la vita privata di lavoratori e di terzi, l'utilizzo delle risorse informatiche messe a disposizione del personale deve sempre ispirarsi ai principi di diligenza e correttezza, atteggiamenti richiesti nello svolgimento di ogni atto o comportamento posto in essere nell'ambito del rapporto di lavoro, in qualsiasi forma esso sia.

La protezione dei dati e delle informazioni nel loro complesso è condizione necessaria per garantire il rispetto dei requisiti di sicurezza che la normativa vigente impone a tutti i soggetti che, a vario titolo, effettuano il trattamento di dati personali.

Il datore di lavoro, inoltre, deve assicurare la funzionalità e il corretto impiego degli strumenti informatici da parte dei lavoratori.

Il presente regolamento, quindi, persegue le seguenti finalità:

- adottare indirizzi trasparenti, capaci di comunicare con estrema chiarezza al lavoratore le corrette modalità di utilizzo degli strumenti informatici assegnatigli per lo svolgimento delle mansioni attribuite;
- definire con altrettanta chiarezza il diritto dell'Amministrazione a verificare l'uso corretto dei suddetti strumenti;
- individuare le modalità con cui l'Amministrazione esercita tale diritto di verifica;
- evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza dei dati.

Indice

Art. 1. Campo di applicazione del regolamento

Art. 2. Amministrazione delle Risorse Informative

Art. 3. Utilizzo del Personal Computer

Art. 4. Gestione e assegnazione delle credenziali di autenticazione

Art. 5. Utilizzo della rete del Comune di FONDI

Art. 6. Utilizzo e conservazione dei supporti rimovibili

Art. 7. Utilizzo di PC portatili

Art. 8. Uso della posta elettronica

Art. 9. Navigazione in Internet

Art. 10. Protezione antivirus

Art. 11. Utilizzo dei telefoni, fax e fotocopiatrici dell'Ente

Art. 12. Osservanza delle disposizioni in materia di Privacy

Art. 13. Accesso ai dati trattati dall'utente

Art. 14. Sistema di controllo

Art. 15. Sanzioni e deroghe

Art. 16. Aggiornamento e revisione

Art. 17. Entrata in vigore del regolamento e pubblicità

ART. 1
CAMPO DI APPLICAZIONE DEL REGOLAMENTO

1.1 Il nuovo regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori del Comune di Fondi a prescindere dal rapporto contrattuale con la stessa intrattenuto (collaboratori a progetto, in stage, ecc.), a tutti gli Amministratori (Consiglieri comunali, Assessori, ecc.) che abbiano accesso alla Rete del Comune di FONDI, costituita dall'insieme delle Risorse informatiche, cioè dalle Risorse infrastrutturali e dal patrimonio informativo digitale. Le Risorse infrastrutturali sono le componenti hardware/software e gli apparati elettronici collegati alla Rete Informatica comunale. Il Patrimonio informativo è l'insieme delle banche dati in formato digitale e in generale tutti i documenti prodotti tramite l'utilizzo dei suddetti apparati.

1.2 Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi chiunque, dirigente, dipendente o collaboratore (collaboratore a progetto, in stage, ecc.) in possesso di specifiche credenziali di autenticazione. Tale figura potrà anche venir indicata quale "incaricato del trattamento". Per "utente", deve altresì intendersi, anche l'Amministratore (Consigliere Comunale, Assessore, ecc.) che anche saltuariamente ha accesso alle risorse informatiche e telematiche per svariate ragioni.

1.3 È fatto altresì obbligo di notifica del presente Regolamento a tutti i fornitori e manutentori (hardware e software) delle apparecchiature informatiche comunali.

ART. 2
AMMINISTRAZIONE DELLE RISORSE INFORMATIVE

2.1 Il Dirigente del Settore n.1 nomina, ove non vi abbia già provveduto, il Responsabile del Centro Elaborazione Dati (Amministratore di Sistema).

L'Amministratore di sistema nominato dal Dirigente del settore N. 1 ai sensi del codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n.196 e s.m.i.) e del provvedimento del garante del 24 dicembre 2008, n.300, si occupa di implementare e assicurare la manutenzione in efficienza delle postazioni di lavoro e dei servizi informatizzati forniti dall'Ente e di implementare le misure atte a garantire la sicurezza e l'integrità delle risorse informatiche dell'Ente (software, hardware, dati).

Nell'esercizio dei suoi compiti l'Amministratore di sistema può in qualsiasi momento avere la necessità di accedere alle postazioni di lavoro, alle caselle di posta elettronica e ai dati su server di dipendenti e collaboratori e questo di norma avverrà alla presenza della persona interessata o previa acquisizione del suo consenso.

L'Amministratore di sistema può inoltre svolgere attività di monitoraggio della posta elettronica e del flusso dati attraverso la rete dell'amministrazione comunale, finalizzata alla ricerca di eventuali minacce alla sicurezza o anomalie nel funzionamento dei servizi che si dovessero verificare, senza dover dare preavviso della propria attività. L'amministratore di sistema in particolare può:

a) Gestire hardware/software di tutte le strutture tecniche informatiche di appartenenza del Comune di FONDI, collegate in rete o meno.

b) Gestire esecutivamente (creazione, attivazione, disattivazione e tutte le relative attività amministrative) gli account di rete e i relativi privilegi di accesso alle risorse, assegnati agli utenti della Rete Informatica comunale secondo quanto stabilito da ogni Dirigente.

c) Monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare il

corretto utilizzo delle risorse di rete, dei computer e degli applicativi, solo se rientrante 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.

d) Creare, modificare, rimuovere o utilizzare qualunque account o privilegio, solo se rientrante 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.

e) Rimuovere programmi software dalle risorse informatiche assegnate agli utenti, solo se rientrante 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.

f) Rimuovere componenti hardware dalle risorse informatiche assegnate agli utenti, solo se rientranti nelle normali attività di manutenzione, gestione della sicurezza e di protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori.

g) Utilizzare le credenziali di accesso di amministrazione del sistema, o l'account di un utente tramite reinizializzazione della relativa password, per accedere ai dati o alle applicazioni presenti su una risorsa informatica assegnata a un utente in caso di prolungata assenza, irrintracciabilità o impedimento dello stesso. Tale utilizzo deve essere esplicitamente richiesto dal Dirigente del Settore dell'utente assente o impedito e deve essere limitato al tempo strettamente necessario al compimento delle attività indifferibili per cui è stato richiesto.

2.2 Il Responsabile del Centro Elaborazione Dati si attiene alle disposizioni impartite dal Dirigente del Settore n. 1 e ha l'onere di segnalare a quest'ultimo qualunque infrazione che minacci la sicurezza della Infrastruttura e il patrimonio informativo comunale, nonché le violazioni del presente Regolamento e delle norme in materia.

2.3 Il Responsabile del Centro Elaborazione Dati coordina le unità operative applicate, gli interventi tecnici dei fornitori, dei prestatori di servizi e ogni attività del Sistema Informativo relazionando al Dirigente del Settore n.1.

2.4 Il Responsabile del Centro Elaborazione Dati deve verificare settimanalmente che i sistemi antivirus centralizzati siano perfettamente operativi.

ART. 3
UTILIZZO DEL PERSONAL COMPUTER

3.1 Il Personal Computer affidato all'utente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire a innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza dell'Infrastruttura e dei dati. Il personal computer deve essere custodito con cura evitando ogni possibile forma di danneggiamento.

3.2 Il personal computer dato in affidamento all'utente permette l'accesso alla rete del Comune di Fondi solo attraverso specifiche credenziali di autenticazione come meglio descritto al successivo punto 4 del presente Regolamento.

3.3 Il Comune di Fondi rende noto che il personale incaricato che opera presso il Settore n. 1 - Servizio C.E.D. è autorizzato a compiere interventi nel Sistema Informatico dell'Ente, diretti a garantire la sicurezza e la salvaguardia del Sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi, ad es. aggiornamento, sostituzione, implementazione di programmi, manutenzione

hardware ecc.). Detti interventi, in considerazione dei divieti di cui ai successivi punti nn. 8.2 e 9.1, potranno anche comportare l'accesso in qualunque momento ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, nonché alla verifica sui siti internet acceduti dagli utenti abilitati alla navigazione esterna. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'Ente, si applica anche in caso di assenza prolungata o impedimento dell'utente.

3.4 Il personale incaricato del C.E.D. ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, ecc. L'intervento viene effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.

3.5 Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal personale del C.E.D. per conto del Comune di Fondi né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione espone l'Amministrazione comunale a gravi responsabilità civili. Si evidenzia inoltre, che le violazioni della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato, vengono sanzionate anche penalmente. A tal proposito, il personale del C.E.D., procederà come previsto al successivo punto 5.6 del presente Regolamento.

3.6 Salvo preventiva espressa autorizzazione del personale del C.E.D., non è consentito all'utente modificare le caratteristiche impostate sul proprio PC né procedere a installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ecc.).

3.7 Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale del C.E.D., nel caso in cui siano rilevati virus non rimossi dal sistema centralizzato, e adottando quanto previsto dal successivo punto 10 del presente Regolamento relativo alle procedure di protezione antivirus.

3.8 Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo. In ogni caso, 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. A tal proposito, il personale del C.E.D., può adottare procedure remote automatiche di arresto del personal computer .

3.9 Ogni tipo di intervento su apparecchiature informatiche che possano interessare o influenzare la rete LAN, i Server, i singoli personal computer, inotebook, le stampanti di rete, ecc. dovranno obbligatoriamente essere comunicati formalmente al personale del C.E.D. con il quale saranno concordati tempi e modi d'intervento, previa autorizzazione del Dirigente del Settore.

ART.4
GESTIONE E ASSEGNAZIONE DELLE CREDENZIALI DI AUTENTICAZIONE

4.1 Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dal personale del C.E.D., previa formale richiesta del Dirigente o Responsabile del Settore, nell'ambito del quale verrà inserito e andrà a operare il nuovo utente. Nel caso di collaboratori a progetto, ecc., la preventiva richiesta verrà inoltrata direttamente dal Responsabile dell'ufficio con il quale il

collaboratore si coordina nell'espletamento del proprio incarico.

4.2 Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id o account), assegnato dal Settore n. 1 – Servizio C.E.D., associato a una parola chiave (password) riservata che dovrà essere sostituita obbligatoriamente al primo accesso dall'operatore. Le credenziali di accesso sono strettamente personali e non devono essere comunicate ad alcuno. Non sono previste eccezioni. Non è consentita l'attivazione della password di accensione (BIOS).

4.3 La parola chiave, formata da lettere (maiuscole o minuscole) e/o numeri, anche in combinazione fra loro, deve essere composta da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato.

4.4 È necessario procedere alla modifica della parola chiave a cura dell'utente, incaricato del trattamento, oltre che al primo utilizzo (punto 3.2), successivamente almeno ogni sei mesi (ogni tre mesi nel caso invece di trattamento di dati sensibili attraverso l'ausilio di strumenti elettronici), qualora non imposta dal sistema informatizzato.

4.5 Qualora la parola chiave dovesse essere sostituita, per decorso del termine sopra previsto e/o in quanto abbia perduto la propria riservatezza, si procederà in tal senso d'intesa con il personale del C.E.D., al quale dovrà essere inoltrata precisa istanza motivata.

ART.5
UTILIZZO DELLA RETE

5.1 Nel rispetto dei principi di trasparenza, collaborazione e condivisione, previsti dalla normativa vigente in materia, ogni Dirigente, reciprocamente, metterà a disposizione della struttura le banche dati digitali di propria competenza.

5.2 Al fine di favorire il processo di riordino e di riduzione degli adempimenti amministrativi, nel rispetto della Legge 241/90 e del DPR 445/2000, gli uffici pubblici comunali hanno l'obbligo di accedere ai sistemi informativi delle diverse ripartizioni al fine di estrarre copia di documenti e atti autorizzatori, di cui lo stesso Ente ne rilascia gli originali.

5.3 Il Sistema Informativo del Comune Fondi è strutturato nel cosiddetto "dominio locale" cui ogni personal computer è connesso per mezzo della rete LAN o WAN. Dette regole (policy) garantiscono la sicurezza della rete informativa comunale e la condivisione delle informazioni; pertanto, ogni apparecchiatura informatica e l'utente che ne fa uso sono soggetti a tali regole. Solo eventuali difficoltà tecnico-operative, o esigenze temporanee, valutate dal Responsabile del Centro Elaborazione Dati, possono derogarvi.

5.4 Per l'accesso alla rete del Comune di Fondi ciascun utente deve essere in possesso della specifica credenziale di autenticazione.

5.5 È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato. Le parole chiave d'ingresso alla rete e ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.

5.6 Per motivi di sicurezza, è assolutamente vietato connettere autonomamente nuove apparecchiature informatiche (personal computer, notebook, stampanti di rete, ecc.) alla rete LAN comunale. Dette operazioni dovranno essere obbligatoriamente concordate con il personale del

C.E.D., previa richiesta del Dirigente afferente l'Ufficio comunale interessato, al Dirigente del Settore n. 1 Informatico che autorizzerà o meno le operazioni richieste.

5.7 Le cartelle utenti presenti nei server e le banche dati digitali del Comune di Fondi sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non riguardi l'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità vengono svolte regolari attività di controllo, amministrazione e backup da parte del personale del C.E.D. Si ricorda che tutti i dischi o altre unità di memorizzazione locali (es. disco C: interno PC) non sono soggetti a salvataggio da parte del personale incaricato del C.E.D. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo utente.

5.8 Il personale del C.E.D. può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete, nonché alla rimozione di ogni altra applicazione diversa da quella ufficialmente installata dal personale incaricato del C.E.D., non licenziata o non pertinente l'attività lavorativa.

5.9 Al fine di migliorare le prestazioni e la sicurezza del Sistema Informativo comunale, nonché del singolo PC o notebook collegati alla rete LAN, il personale del C.E.D., predisporrà le procedure remote necessarie alla rimozione di software inutili e/o non strettamente legati all'attività lavorativa.

5.10 Per motivi di sicurezza, il personale del C.E.D., predisporrà le procedure necessarie a inibire l'accesso alla rete LAN degli utenti oltre l'orario ordinario di servizio. Particolari esigenze dovranno essere formalmente comunicate al suddetto servizio.

5.11 Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

ART.6
UTILIZZO E CONSERVAZIONE DEI SUPPORTI RIMOVIBILI

6.1 Tutti i supporti magnetici rimovibili (dischetti, CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati sensibili o riservati, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.

6.2 Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, ciascun utente dovrà contattare il personale del C.E.D. e seguire le istruzioni da questo impartite.

6.3 In ogni caso, i supporti magnetici contenenti dati sensibili devono essere adeguatamente custoditi dagli utenti in armadi chiusi.

6.4 È vietato l'utilizzo di supporti rimovibili personali.

6.5 L'utente è responsabile della custodia dei supporti e dei dati aziendali in essi contenuti.

ART. 7
UTILIZZO DI PC PORTATILI (NOTEBOOK)

7.1 L'utente è responsabile del PC portatile di cui ha la disponibilità e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

7.2 Ai PC portatili si applicano le regole di utilizzo previste dal presente regolamento, con particolare attenzione alla rimozione di eventuali file elaborati prima della riconsegna.

7.3 I PC portatili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari, per evitare danni o sottrazioni.

7.4 Tali disposizioni si applicano anche nei confronti di incaricati esterni, ecc.

ART. 8
USO DELLA POSTA ELETTRONICA

8.1 La casella di posta elettronica assegnata all'utente è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

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

a) l'invio e/o la ricezione di allegati contenenti filmati o brani musicali (es. mp3, ecc.) non legati all'attività lavorativa;

b) l'invio e/o la ricezione di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list, ecc.;

c) la partecipazione a catene telematiche. Se si dovessero peraltro ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al personale del C.E.D.
Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.

d) la trasmissione a mezzo di posta elettronica di dati sensibili, confidenziali e personali di alcun genere, salvo i casi espressamente previsti dalla normativa vigente in materia di protezione dei dati personali (D.Lgs. 196 del 30/6/2003 e s.m.i.).

e) Inoltrare e/o inviare messaggi di posta elettronica all'interno del Comune di Fondi non pertinenti l'attività lavorativa o contenenti allegati di notevole dimensione.

f) Inviare tramite posta elettronica user-id, password, configurazioni della rete interna, indirizzi e nomi dei sistemi informatici.

8.3 La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

8.4 Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali del Comune di Fondi, ovvero contenga documenti da considerarsi

riservati, deve essere visionata o autorizzata dal Dirigente del Settore.

8.5 È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario. Si evidenzia però che le comunicazioni ufficiali, da inviarsi mediante gli strumenti tradizionali (fax, posta, ...), devono essere autorizzate e firmate dal Dirigente del Settore e/o dai Responsabili di Ufficio, a seconda del loro contenuto e dei destinatari delle stesse.

8.6 È obbligatorio porre la massima attenzione nell'aprire i file allegati di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

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

8.8 In caso di assenza non programmata (ad es. per malattia) la procedura qualora non possa essere attivata dal lavoratore avvalendosi del servizio webmail entro due giorni - verrà attivata dall'Ente purché comunicata per iscritto, a cura del Dirigente del Settore di riferimento, al Settore n. 1 – Servizio C.E.D.

8.9 Sarà comunque consentito al superiore gerarchico dell'utente o, comunque, sentito l'utente, a persona individuata dall'azienda, accedere alla casella di posta elettronica dell'utente per ogni ipotesi in cui si renda necessario (ad es.: mancata attivazione della funzionalità di cui al punto 8.7; assenza non programmata e impossibilità di attendere i due giorni di cui al punto 8.8).

8.10 Il personale del C.E.D., nell'impossibilità di procedere come sopra indicato e nella necessità di non pregiudicare la necessaria tempestività ed efficacia dell'intervento, potrà accedere alla casella di posta elettronica per le sole finalità indicate al punto 3.3.

8.11 Al fine di ribadire agli interlocutori la natura esclusivamente aziendale della casella di posta elettronica, i messaggi possono contenere un avvertimento standardizzato nel quale sia dichiarata la natura non personale dei messaggi stessi.

8.12 Tutti i messaggi di posta elettronica sono soggetti a scansione antivirus. Il sistema Informatizzato, a tutela della propria integrità, procederà alla rimozione di eventuali allegati sospetti. Qualora risulti impossibile ricevere allegati di posta elettronica, è necessario comunicarlo al personale del C.E.D. il quale, previa richiesta scritta, valuterà la possibilità di download del file allegato.

ART. 9
NAVIGAZIONE SU INTERNET

9.1 Il PC assegnato al singolo utente, eventualmente abilitato alla navigazione in Internet, costituisce uno strumento dell'Ente utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa.

9.2 In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare internet per:

a) l'upload o il download di software gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa (filmati e musica) e previa verifica dell'attendibilità dei siti in questione (nel caso di dubbio, dovrà essere contattato, a tal fine, il personale del C.E.D.);

b) effettuare ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dal Dirigente del Settore e comunque nel rispetto delle normali procedure di acquisto;

c) ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;

d) la partecipazione a Forum non professionali, l'utilizzo di chat line, di bacheche elettroniche, facebook, myspace e qualunque registrazione sulla rete internet anche utilizzando pseudonimi (o nickname) se non espressamente autorizzati dal Dirigente del Settore;

e) l'accesso, tramite internet, a caselle webmail di posta elettronica personale non preventivamente autorizzate.

9.3 Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa del Comune di Fondi, si rende nota l'adozione di uno specifico sistema di blocco o filtro automatico che previene determinate operazioni quali l'upload o l'accesso a determinati siti inseriti in una black list gestiti da idonea strumentazione (firewall, proxy server, ecc.).

9.4 Gli eventuali controlli, compiuti dal personale incaricato del ai sensi del precedente punto 3.3, potranno eseguirsi mediante un sistema di controllo dei contenuti (Proxy server, ecc.) o mediante "file di log" della navigazione svolta. I file di log vengono conservati nel pieno rispetto delle disposizioni in materia di privacy e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori.

ART. 10
PROTEZIONE ANTIVIRUS

10.1 Il sistema informatico del Comune di Fondi è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informativo comunale mediante virus o mediante ogni altro software aggressivo.

10.2 Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer, nonché segnalare prontamente l'accaduto al personale del C.E.D., qualora il virus non risulti rimosso.

10.3 Ogni dispositivo magnetico di provenienza esterna all'Azienda dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al personale del C.E.D., qualora il virus non risulti rimosso.

ART. 11
UTILIZZO DEI TELEFONI, FAX E FOTOCOPIATRICI AZIENDALI

11.1 Il telefono aziendale affidato all'utente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti l'attività lavorativa stessa. La ricezione o l'effettuazione di telefonate personali è consentito solo nel caso di comprovata necessità e urgenza, mediante il telefono fisso aziendale a disposizione.

11.2 Qualora venisse assegnato un cellulare aziendale all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Al cellulare aziendale si applicano le medesime regole sopra previste per l'utilizzo del telefono aziendale: in particolare è vietato l'utilizzo del telefono cellulare messo a disposizione per inviare o ricevere SMS o MMS di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa. L'eventuale uso promiscuo (anche per fini personali) del telefono cellulare aziendale è possibile soltanto in presenza di preventiva autorizzazione scritta e in conformità delle istruzioni al riguardo impartite dal Dirigente del Settore.

11.3 È vietato l'utilizzo dei fax aziendali per fini personali, tanto per spedire quanto per ricevere documentazione, salva diversa esplicita autorizzazione da parte del Dirigente del Settore.

11.4 È vietato l'utilizzo delle fotocopiatrici aziendali per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Dirigente del Settore.

ART. 12
OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY

12.1 È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, come indicato nella lettera di designazione dell'incaricato del trattamento dei dati ai sensi del Disciplinare tecnico allegato al D. Lgs. n. 196/2003e s.m.i.

ART. 13
ACCESSO AI DATI TRATTATI DALL'UTENTE

13.1 Oltre che per motivi di sicurezza del sistema informativo, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento, sostituzione, implementazione di programmi, manutenzione hardware, ecc.) o per finalità di controllo e programmazione dei costi dell'Ente (ad esempio, verifica costi di connessione a internet, traffico telefonico, ecc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà della Dirigenza dell'Ente, accedere tramite il Dirigente del Settore n. 1 ed il personale del C.E.D. o addetti alla manutenzione, nel rispetto della normativa sulla privacy e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori, a tutti gli strumenti informatici aziendali e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico.

ART. 14
SISTEMI DI CONTROLLO

14.1 A garanzia della sicurezza dei sistemi informativi e dei servizi di rete, è nella facoltà dell'Amministrazione effettuare controlli su dati aggregati, riferiti all'intera struttura lavorativa o a

sue aree, nonché predisporre controlli a campione, in forma anonima, sugli accessi ad Internet e sulla navigazione web.

14.2 È sempre fatta salva l'ipotesi dell'attivazione di controlli, anche individualizzati, che trovino giustificazione nella necessità di corrispondere ad eventuali richieste di organi di polizia su segnalazione dell'autorità giudiziaria, nel verificarsi di un evento dannoso o una situazione di pericolo che richieda un immediato intervento o nella presenza di sospetti relativamente all'esistenza di condotte improprie nell'uso delle apparecchiature (cd. controlli difensivi).

14.3 Per motivi di sicurezza e protezione dei dati, ogni attività compiuta nella rete Informatica può essere sottoposta a registrazione in appositi file e riconducibili, indirettamente, all'utente. Detti file possono essere soggetti a trattamento solo per fini istituzionali, per attività di monitoraggio e controllo e possono essere messi a disposizione dell'Autorità Giudiziaria in caso di accertata violazione delle norme vigenti. La riservatezza delle informazioni è soggetta a quanto dettato dal D. Lgs. 196/2003 e s.m.i. e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori.

14.4 L'Amministrazione comunale è dotata di un sistema di filtraggio dei contenuti accessibili via internet, che precluderà dall'adozione del presente regolamento l'accesso a determinate categorie di risorse per la loro non attinenza alle attività istituzionali e per garantire a tutti la fruibilità e la sicurezza di internet.
Pertanto, saranno banditi i siti rientranti nelle seguenti categorie:
- Acquisti: Aste/annunci
- Armi/Militari
- Criminalità: Attività illegali
- Criminalità: Estremismo politico/Odio/Discriminazione
- Criminalità: warez/criminalità informatica
- Divertimento/cultura: Musica/radio
- Giochi/gambling
- Malware
- Pornografia/nudità
- Sport
-Tecnologia informatica: anonymous proxies
-Trading-on line e homebanking (l'accesso ai siti di homebanking è consentito a tutti su esplicita autorizzazione del proprio dirigente di assegnazione e attraverso il pc abilitato)
- Violenza/siti estremi
- Social network: Facebook, Myspace, Twitter, Messenger.

14.5 Tali divieti, (ad eccezione dei siti Giochi/gambling, Malware Pornografia/nudità per i quali siti il divieto è esteso anche ai dirigenti) non operano nei confronti dei dirigenti, ai quali è garantito un accesso illimitato, nell'ambito dell'esercizio dei compiti e funzioni e nei confronti di quei dipendenti ai quali per motivi inerenti l'esercizio delle proprie mansioni abbiano avuto specifica autorizzazione all'accesso.

ART. 15
SANZIONI E DEROGHE

15.1 È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente regolamento, a eccezione delle manifeste necessità e dei casi, esclusivamente attestati e motivati dal Dirigente del Settore n. 1 - Servizio C.E.D. con idoneo e formale atto amministrativo. Il mancato rispetto e/o la violazione delle regole sopra ricordate è perseguibile nei confronti del

personale dipendente con provvedimenti disciplinari e/o risarcitori previsti dai vigenti CC.CC.NN.LL., con le modalità ivi previste per il personale dipendente o equiparato, l'applicazione delle sanzioni previste nelle clausole contrattuali per i soggetti non dipendenti nonché con tutte le azioni civili e penali consentite dalle vigenti norme.

ART. 16
AGGIORNAMENTO E REVISIONE

16.1 Il presente Regolamento è soggetto a revisione ogni qualvolta se ne manifesti la necessità.

ART. 17
ENTRATA IN VIGORE DEL REGOLAMENTO E PUBBLICITA'

17.1 Il presente regolamento entra in vigore il 15° giorno dalla pubblicazione all'albo pretorio on-line ed abroga tutte le disposizioni in precedenza adottate in materia.

17.2 Copia del presente regolamento è pubblicato sul sito istituzionale dell'Ente e nell'apposita area condivisa in rete LAN dove ogni utente può visionarlo così da consentirne la massima diffusione e conoscenza.

PUNTO N. 2 ALL'ORDINE DEL GIORNO – REGOLAMENTO PER L'UTILIZZO DEI SISTEMI INFORMATIVI

PRESIDENTE

Cedo la parola al Consigliere Alessandro Sansoni.

CONS. SANSONI

Grazie Presidente, buonasera a tutti. Mi associo agli auguri poc'anzi fatti per l'Assessore Biasillo, e scusatemi se non mi alzo ma avendo più di qualche appunto preferisco fare l'intervento da seduto.

Ebbene volevo partire innanzitutto con i ringraziamenti in special modo al personale del Ced, quindi nella persona di Emilio Nocella che questa sera è qui presente, e a Francesco Bucci, al dirigente del primo settore e non meno importante essendo come posizione per ultimo come ringraziamento al mio caro collega Biagio Coppa che si è occupato dell'implementazione delle ultime in novità legislative che poi hanno appunto composto il regolamento dei sistemi informativi.

Ebbene un'altra cosa che ci terrei a precisare che questa è la prima volta che noi regolamentiamo il settore informatico, direi che è un altro piccolo grande passo anche di questa amministrazione riguardo al metodo di lavoro per l'appunto di regolamentare, razionalizzare il lavoro dell'amministrazione pubblica.

Ebbene se pure vero che in questi anni il processo lavorativo dell'apparato amministrativo ha subito un imponente processo di informatizzazione ragion per cui necessita sempre più una razionalizzazione e soprattutto una più organizzazione dell'apparato informatico in questione.

Tutto questo deve garantire un livello sicuramente di sicurezza e soprattutto di una maggiore formazione da parte di coloro che sono gli utilizzatori dell'apparato informatico stesso.

Ebbene partendo dalle disposizioni della direttiva numero 2 /2009 dove il dipartimento della funzione pubblica ha riepilogato i principi e le regole a cui attenersi per l'utilizzo degli strumenti web quali internet e l'utilizzo della posta elettronica, sul luogo di lavoro garantendo anche le linee guida adottate dal garante per la protezione dei dati personali, con quelli di esercizio di controllo da parte del datore di lavoro appunto per un corretto utilizzo del servizio in questione.

Tale regolamento viene applicato a tutti gli utilizzatori che usufruiscono dell'apparato informatico del Comune, quindi dipendenti, senza distinzione di ruolo e livello, per Consiglieri, Assessori e Sindaco. Con tutte le specifiche credenziali di autenticazione elaborate appunto dal Ced, quindi centro elaborazione dati che sarà per l'appunto la ripartizione principale la quale gestirà queste nuove regolamentazioni che verranno applicate nei prossimi giorni.

Verrà quindi nominato un amministratore di sistema dal dirigente del primo settore, ai sensi del codice in materia di protezione dei dati personali, quindi decreto legislativo del 30 giugno 2003, assieme al provvedimento del garante del dicembre 2008 numero 300. Il quale si occupa di implementare la messa in sicurezza delle postazioni di lavoro dell'apparato informatico stesso.
Ebbene è molto importante anche capire quale sarà l'utilizzo del personal computer, ovvero che deve essere inteso come strumento di lavoro, per cui dovrà essere utilizzato esclusivamente ai fini lavorativi che competono l'utilizzatore, ovviamente non sono ammessi l'utilizzo dei programmi mancanti da autorizzazioni da parte del centro elaborazione dati, quindi Ced, e inoltre personal computer che vengono utilizzati per la navigazione, quindi dalla posta elettronica vengono razionalizzati per l'utilizzo del proprio ambito lavorativo.
Bene un'altra piccola, un piccolo inciso che volevo fare è che comunque in questi due anni e mezzo il Ced ha regolamentato diciamo il livello di protezione di sicurezza, di fatti in questi ultimi due anni e mezzo sono stati installati dei nuovi apparati informatici per quanto riguarda la risoluzione della sicurezza perimetrale che viene quindi intrinseca all'interno di un file il quale provvede in maniera autonoma a ripulire tutta la struttura web dell'apparato comunale e nello stesso tempo per mettere agli utilizzatori del klynd di avere una massima efficienza per l'appunto l'utilizzo quotidiano lavorativo.
Ebbene un altro piccolo passo che ci ha permesso poi di effettuare l'installazione della rete wifi, questo proprio perché attualmente il Ced ha un livello strutturale informatico che permette non solo l'utilizzo della wifi gratuita come sapete che è stata installata nella scorsa estate, ma anche la regolamentazione della stessa permettendo a qualsiasi utilizzatore in questo caso della città di Fondi di usufruire di tutti i suoi servizi.
Un'altra cosa importante è stata poi effettuata la centralizzazione dei salvataggi quindi in tempo reale, questo per permettere quindi l'utilizzo e la, e soprattutto la riservatezza dei dati personali, quindi dati sensibili dell'apparato amministrativo comunale, e ragion per cui anche la centralizzazione della posta elettronica.
I passi successivi che verranno fatti nei prossimi mesi sarà appunto l'installazione del domenin controllory quindi determinerà i tempi di utilizzo dei klynd medesimi e non solo, dando una autenticazione che avrà una specifica per ogni utente il quale avrà un utilizzo univoco che viene poi specificato al nominante, ovverosia il vero utilizzatore del proprio Pc.
Un altro passo importante che verrà fatto è questo, parliamo non solo di tecnologico, ma soprattutto a livello strutturale e economico, ovverosia i terminal service. Grazie a questa regolamentazione noi siamo in grado poi di definire non solo il domein controllery, ma anche l'utilizzo del nuovo apparato informatico, quindi evitando ad esempio dei futuri acquisti quindi del parco macchine perché noi andremo appunto ad utilizzare il terminal service ovverosia centralizzare tutto l'apparato informatico su una unica unità quindi sarà la parte principale del

sistema informatico del centro elaborazione dati, non permettendo più inutili sprechi per i continui rinnovi del parco macchine. Grazie.

PRESIDENTE

Grazie Consigliere Sansoni.

La parola a chi la chiede.

Se non ci sono interventi andiamo subito a votare.

Allora favorevoli per l'approvazione del regolamento per l'utilizzo dei sistemi informatici?

Allora 22 favorevoli. Contrari? Nessuno. Astenuti? 2.

Letto, confermato e sottoscritto

IL PRESIDENTE DEL CONSIGLIO
(prof.ssa Maria Luigia Marino)

IL SEGRETARIO GENERALE
(dott. Francesco Loricchio)

CERTIFICATO DI PUBBLICAZIONE

Il presente verbale viene pubblicato all'albo pretorio On-line di questo Comune secondo le disposizioni legislative vigenti in materia il 15 GEN. 2013 **per restarvi 15 giorni ai sensi di legge.**

Addì 15 GEN. 2013

IL SEGRETARIO GENERALE

DICHIARAZIONE DI ESECUTIVITA'

Il sottoscritto, visti gli atti d'ufficio:

A T T E S T A

Che la presente deliberazione:

- ☐ **E' stata dichiarata immediatamente eseguibile a norma dell'art. 134, 4° comma del T.U. 267/2000**

Addì _____

IL SEGRETARIO GENERALE

(dott. Francesco Loricchio)

PARERI DEI RESPONSABILI DI SERVIZIO
(art. 49 D.Lg.vo 267/2000)

Parere favorevole
in ordine alla regolarità tecnica

IL RESPONSABILE DEL SERVIZIO
(dott.ssa Tommasina Biondino)