CITTÀ DI SESTO SAN GIOVANNI
MEDAGLIA D'ORO AL VALOR MILITARE

Deliberazione della Giunta comunale
N. 89 del 04.04.2012

REGOLAMENTO DI ORGANIZZAZIONE TITOLO VI "USO E GESTIONE DEGLI STRUMENTI INFORMATICI E TELEMATICI". ADOZIONE.

VERBALE

Il 04 aprile 2012 alle ore 15:00 nel palazzo comunale di Sesto San Giovanni, convocata la Giunta comunale, sono intervenuti i Signori:

N. progressivo	Cognome e Nome		Qualifica	Presenze
1	Oldrini	Giorgio	Sindaco	NO
2	Morabito	Demetrio	Vicesindaco	SI
3	Amato	Vincenzo	Assessore	SI
4	Brambilla	Ersilia	Assessore	SI
5	Chittò	Monica	Assessore	NO
6	Pozzi	Alessandro	Assessore	SI
7	Scanagatti	Roberto	Assessore	NO
8	Teormino	Lucia	Assessore	NO
9	Urro	Giovanni	Assessore	SI
10	Zucchi	Claudio	Assessore	SI

Partecipa il Segretario generale Mario Spoto.
In assenza del Sindaco, Giorgio Oldrini, assume la presidenza il Vicesindaco, Demetrio Morabito, che riconosciuta legale l'adunanza dichiara aperta la seduta.

Regolamento di Organizzazione Titolo VI "Uso e gestione degli strumenti informatici e telematici". Adozione

LA GIUNTA COMUNALE

- Vista la relazione del Direttore del Settore Personale e Organizzazione in data 29.3.2012 che costituisce parte integrante del presente atto;
- Atteso che il presente atto è coerente con i programmi indicati nella programmazione pluriennale e annuale, approvati dal Consiglio Comunale, nonché con i compiti e gli obiettivi assegnati al Settore Personale e Organizzazione con i PEG e PDO approvati dalla Giunta Comunale;
- Attesa la competenza della Giunta Comunale ai sensi dell'art.48 del D. Lgs. 267/2000, nonché dell'art.51 comma 3 dello Statuto Comunale in merito all'adozione di regolamenti sull'organizzazione degli uffici e servizi;
- Visto l'art. 4 della Legge 20 maggio 1970 n.300 (Statuto dei Lavoratori);
- Visto il verbale di accordo sottoscritto in data 12.3.2012 con le RSU e le Organizzazioni sindacali CGIL, CISL, UIL e CSA;
- Visti i pareri favorevoli espressi a norma dell'art.49, 1° comma, del D. Lgs. 18 agosto 2000 n.267, come da foglio allegato;
- Richiamato l'articolo l'art. 134, 4° comma, del D. Lgs. citato;
- Con voti unanimi, espressi nelle forme di legge, anche per l'immediata eseguibilità della presente deliberazione

DELIBERA

1. di integrare il vigente Regolamento di Organizzazione con il Titolo VI "Uso e gestione degli strumenti informatici e telematici", composto dagli articoli da 63 a 77, nonché dalla norma finale art.78, come da allegato;

2. di abrogare il vigente art.63 "Norma transitoria e finale", che viene sostituito con il nuovo art.78 "Entrata in vigore, aggiornamento e revisione, Norma finale";

3. di dare atto che il presente Titolo VI "Uso e gestione degli strumenti informatici e telematici" che andrà ad integrare il Regolamento di Organizzazione è frutto di un accordo sottoscritto in data 12.3.2012 con le RSU e le Organizzazioni Sindacali CGIL, CISL, UIL e CSA;

4. di dichiarare la presente deliberazione immediatamente eseguibile ai sensi dell'art.134, 4° comma, del D. Lgs. 18 agosto 2000 n.267.

RELAZIONE

Il Comune di Sesto San Giovanni dispone di una articolata rete informatica costituita da risorse informatiche e telematiche, da risorse infrastrutturali e dal patrimonio informativo digitale.
Le risorse infrastrutturali sono le componenti hardware/software e le apparecchiature elettroniche collegate alla rete informatica comunale, il patrimonio informativo è l'insieme delle banche dati in formato digitale ed in generale tutti i documenti prodotti tramite l'utilizzo dei suddetti apparati.

La rete informatica comunale è uno strumento indispensabile per perseguire le finalità dell'amministrazione comunale e va quindi adottata ogni misura, organizzativa e tecnologica, volta a prevenire il rischio di utilizzi impropri delle strumentazioni e delle banche dati di proprietà del Comune.

E' necessario in particolare assicurare un corretto utilizzo dei sistemi e delle apparecchiature nel rispetto delle leggi, norme ed obblighi contrattuali da parte dei dipendenti e degli amministratori abilitati nel rispetto dei diritti degli stessi e di terzi cittadini in particolare il diritto alla riservatezza.

Va considerato che le risorse informatiche comunali sono un patrimonio importantissimo che va protetto e mantenuto in efficienza, attraverso un corretto utilizzo e una adeguata manutenzione.

Occorre quindi adottare delle norme regolamentari che definiscano chiare e corrette procedure e allo scopo è stato redatto l'allegato articolato che si propone all'approvazione della Giunta Comunale quale nuovo Titolo del vigente Regolamento di organizzazione.

La regolamentazione proposta prevede la possibilità da parte dei Responsabili dei Settori e del Settore servizi informativi di accedere direttamente o in remoto sui computer e sulle banche dati di proprietà comunale gestiti ed elaborati dai dipendenti e dagli amministratori per ragioni operative e manutentive, tali interventi potrebbero concretarsi come controlli a distanza dell'attività dei lavoratori pertanto si è ritenuto necessario sottoporre l'articolato regolamentare alle rappresentanze sindacali aziendali per l'accordo previsto dall'art. 4 della Legge 20 maggio 1970 n.300 (Statuto dei Lavoratori).

Le RSU e le Organizzazioni Sindacali CGIL, CISL, UIL e CSA in data 12.3.2012 hanno sottoscritto l'accordo sull'allegato Titolo VI "Uso e gestione degli strumenti informatici e telematici" che integrerà il vigente Regolamento di organizzazione. Contestualmente all'integrazione viene abrogato l'art.63 "Norma transitoria e finale" che viene sostituito dal nuovo art. 78 "Entrata in vigore, aggiornamento e revisione, Norma finale."

Sesto San Giovanni, 29.3.2012

Il Direttore del Personale e dell'Organizzazione
Sergio Melzi

TITOLO VI
USO E GESTIONE DEGLI STRUMENTI INFORMATICI E TELEMATICI

Art. 63
"Oggetto ed ambito di applicazione"

1. Il presente titolo disciplina l'uso e la gestione da parte degli amministratori e dipendenti del Comune di Sesto San Giovanni degli strumenti informatici e telematici dell'Ente (PC, notebook, telefonini palmari e similari), nell'ambito dello svolgimento delle proprie mansioni e compiti, ai fini di un corretto utilizzo degli strumenti stessi.

2. La rete del Comune di Sesto San Giovanni è costituita dall'insieme di tutte le risorse informatiche e telematiche, cioè dalle risorse infrastrutturali e dal patrimonio informativo digitale.
   Le risorse infrastrutturali sono le componenti hardware/software (apparecchiature che costituiscono il computer/programmi informatici) e le apparecchiature elettroniche collegate alla rete informatica comunale.
   Il patrimonio informativo è l'insieme delle banche dati in formato digitale ed in generale tutti i documenti prodotti tramite l'utilizzo dei suddetti apparati.

3. Il presente regolamento si applica a tutti gli utenti interni autorizzati ad accedere alla rete comunale.
   Per utenti interni si intendono gli amministratori, i dirigenti, i dipendenti, a tempo indeterminato e determinato, ed i collaboratori coordinati e continuativi.

Art. 64
"Principi generali"

1. L'Amministrazione promuove l'uso delle apparecchiature informatiche e telematiche e della rete quale strumenti utili per perseguire le proprie finalità e persegue ogni opportuna misura, organizzativa e tecnologica, volta a prevenire il rischio di utilizzi impropri delle strumentazioni e delle banche dati di proprietà del Comune.

2. Gli utenti manifestano liberamente il proprio pensiero nel rispetto dei diritti degli altri utenti e di terzi, nel rispetto dell'integrità dei sistemi e delle relative risorse fisiche, in osservanza delle leggi, norme ed obblighi contrattuali.

3. Consapevoli delle potenzialità offerte dagli strumenti informatici e telematici, gli utenti si impegnano ad agire con responsabilità ed a non commettere abusi aderendo ad un principio di autodisciplina.

4. Nell'ambito di una preventiva programmazione del fabbisogno e delle risorse disponibili a Bilancio, d'intesa tra il Settore Sistemi Informativi (SSI) e le Direzioni di riferimento, il posto di lavoro, costituito dal personal computer e da tutti i necessari servizi, viene consegnato completo di quanto necessario per svolgere le proprie funzioni, ed è pertanto vietato modificarne la configurazione, salvo che all'utente non siano stati assegnati i diritti di amministratore.

5. Il software installato sui personal computer, licenziato e configurato a cura del personale incaricato del SSI, è quello richiesto dalle specifiche attività lavorative dell'operatore. E' pertanto successivamente proibito installare qualsiasi programma da parte dell'utente o di altri operatori, escluso l'amministratore del sistema.

6. Ogni utente ha la responsabilità civile, penale e amministrativa (disciplinare e contabile) del corretto uso delle risorse informatiche e telematiche, dei servizi/programmi a cui ha accesso e dei dati trattati a fini istituzionali.
   E' altresì responsabile del contenuto delle comunicazioni effettuate e ricevute a fini istituzionali anche per quanto attiene la riservatezza dei dati ivi contenuti, la cui diffusione impropria potrebbe configurare violazione del segreto d'ufficio o della normativa per la tutela dei dati personali.
   Sono vietati comportamenti che possono creare danno, anche di immagine, all'Ente.

7. L'utilizzo delle risorse informatiche e telematiche non deve compromettere la sicurezza e la riservatezza del sistema informativo, né pregiudicare ed ostacolare le attività dell'Amministrazione, né essere destinato al perseguimento di interessi privati.

8. Il lavoratore deve avere cura ed utilizzare gli strumenti informatici, internet, posta elettronica e servizi di telefonia in modo appropriato e diligente ed è responsabile della propria postazione di lavoro, evitando ogni possibile forma di danneggiamento.

9. Il dipendente ha, altresì l'obbligo di impedire ad altri indebiti utilizzi della propria apparecchiatura informatica, non rilevando, al fine del difetto di responsabilità, il fatto che altri, in sua assenza, abbiano potuto usare la propria postazione lavorativa.

10. Ogni utente è responsabile dei dati lavorativi memorizzati nel proprio personal computer. Per questo motivo è tenuto ad effettuare la copia di questi dati secondo le indicazioni dei rispettivi Direttori per quanto riguarda gli aspetti relativi alle materie di competenza e del Direttore del SSI per gli aspetti tecnico-informatici.

11. Il Responsabile/Dirigente di ogni Servizio/Settore, nell'ambito delle proprie prerogative di vigilanza circa il corretto utilizzo delle risorse assegnate, può avvalersi del supporto tecnico del Settore Sistemi Informativi.

Art. 65
"Utilizzo del personal computer"

1. Il personal computer, affidato all'utente, è uno strumento di lavoro: il suo utilizzo deve essere finalizzato esclusivamente allo svolgimento dell'attività lavorativa al fine di non contribuire ad innescare inutili disservizi, costi di manutenzione e minacce alla sicurezza.

2. E' consentito, in via eccezionale, un utilizzo limitato del personal computer per scopi personali, secondo le norme dettate dal presente regolamento, prevalentemente durante la pausa o per improrogabili esigenze straordinarie e del tutto occasionali.
   Il personal computer deve essere utilizzato con cura evitando ogni possibile forma di danneggiamento.

3. Il personal computer viene assegnato al Settore di appartenenza e per questo affidato in uso al dipendente (dipendenti, in caso di "sportelli di servizio" o "postazioni condivise"), in relazione alle funzioni svolte nell'ambito del rispettivo Settore di appartenenza, incrementandone la rispettiva dotazione strumentale.
   Nell'ambito di una preventiva programmazione del fabbisogno, d'intesa con il Settore Sistemi Informativi, e delle risorse disponibili a bilancio, la richiesta deve essere tempestivamente fatta dal relativo Responsabile/Dirigente di riferimento.

4. In caso di cessazione/trasferimento del dipendente e/o modifiche delle esigenze, occorre prontamente comunicare ogni variazione al Settore Sistemi Informativi per i necessari interventi: variazioni d'utente, applicazioni ed eventuale recupero dati.
   Salvo diverse e motivate intese, il personal computer resta in dotazione allo stesso Settore di appartenenza nel caso di effettiva sostituzione del personale; rimesso invece a disposizione del Settore Sistemi Informativi per altre assegnazioni, in caso contrario.

5. Il personal computer dato in affidamento all'utente permette l'accesso alla Rete del Comune di Sesto San Giovanni solo attraverso specifiche credenziali di autenticazione, (user, ovvero il nome dell'utente, e password, parola che consente all'utente l'accesso - *usr e pwd -),* come meglio descritto al successivo art. 66 del presente Regolamento.

6. Al fine di evitarne l'utilizzo da parte di terzi e l'indebito uso, è necessario chiudere tutte le applicazioni attive e spegnere fisicamente il Personal Computer al termine dell'attività lavorativa, ogni sera, prima di lasciare gli uffici, o in caso di assenze prolungate o di suo inutilizzo.
   In caso di brevi assenze è comunque necessario chiudere le applicazioni e proteggerne l'accesso anche con l'uso di salvaschermo (screen saver) automatico dotato di password, ed estrarre e custodire eventuali supporti removibili e ogni ulteriore hardware di autenticazione.

7. Non è possibile modificare le configurazioni hardware e software predefinite dagli amministratori di sistema ed installare autonomamente programmi o applicativi senza preventiva autorizzazione.

8. Non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica, salvo si tratti di documenti da utilizzare nei procedimenti.

9. Il personale del Settore Sistemi Informativi, incaricato della gestione e della manutenzione dei componenti del sistema informatico e della rete (Amministratori di Sistema) può, in qualsiasi momento, procedere alla rimozione di ogni file o applicazione che riterrà essere pericoloso per la sicurezza, sia sui singoli personal computer, sia sulle unità di rete, previa informazione agli utenti interessati.

10. Il personale del Settore Sistemi Informativi, incaricato della gestione e della manutenzione dei componenti del sistema informatico e della rete (Amministratori di Sistema) può accedere al personal computer (anche con strumenti di supporto, assistenza e diagnostica remota) per manutenzione preventiva e correttiva, previa informazione all'utente interessato.

Art. 66
"Gestione ed assegnazione delle credenziali di autenticazione"

1. Le credenziali di autenticazione per l'accesso alla rete vengono assegnate ad ogni utente dal personale incaricato del Settore Sistemi Informativi, previa preventiva richiesta del Responsabile/Dirigente del Servizio/Settore nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente nell'espletamento del proprio incarico (specifici programmi software e relativi requisiti).

2. Le credenziali di autenticazione (*account*) consistono in un codice identificativo personale (*username* o *user id*) per l'identificazione dell'utente e da una parola chiave (*pwd* o *password*) riservata, che dovrà essere custodita dall'incaricato con la massima diligenza e non divulgata. Non è consentita l'attivazione della password di accensione (*bios*), senza preventiva autorizzazione da parte del personale incaricato del Settore Sistemi Informativi.

3. Si distinguono account di accesso al personal computer ed alla rete e di accesso ai programmi autorizzati, ciascuno con una specifica password, in particolare:
   - unico account di rete, per l'avvio e l'utilizzo del sistema operativo e di tutte le risorse di rete;
   - più account per l'accesso ai programmi, agli applicativi ed alla posta elettronica.

   Per incrementare il livello di sicurezza, l'Amministrazione Comunale adotterà progressivamente l'utilizzo di sistemi di autenticazione unica o identificazione unica ("single sign on") ovvero sistemi specializzati che consentono ad un utente del sistema informatico

di autenticarsi una sola volta alla rete e di accedere a tutte le risorse, a tutti gli applicativi ed a tutti i servizi informatici a cui è abilitato.

4. La parola chiave (*password*), formata da lettere (maiuscole o minuscole), numeri e caratteri speciali, anche in combinazione fra loro, deve essere composta da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato, evitando anche contenuti di senso logico immediato facilmente individuabili.

5. È necessario procedere alla modifica delle parole chiave a cura dell'utente, incaricato del trattamento, al primo utilizzo e, successivamente, almeno ogni 3 mesi sia per i dati comuni che per quelli sensibili e giudiziari.

6. L'Utente non deve lasciare incustodito ed accessibile l'apparecchiatura durante l'attività lavorativa, anche mediante l'attivazione automatica del salva schermo (*Screen Saver)* dopo alcuni minuti di inattività e la sua protezione con password (Password d'Utente). Al termine dell'attività lavorativa occorre scollegarsi da ogni applicazione e spegnere l'apparecchiatura.

7. Qualora la parola chiave dovesse venir sostituita, in caso di perdita/dimenticanza, per decorso del termine sopra previsto e/o in quanto abbia perduto la propria riservatezza, il dipendente "titolare" (*user*) deve darne comunicazione al Settore Sistemi Informativi (tramite l'assistenza normalmente erogata) e richiederne la tempestiva sostituzione.
   Il SSI "forzerà" una nuova password d'utente da ri-personalizzare a cura dello stesso utente al primo collegamento.

8. In caso di prolungata assenza del singolo dipendente, qualora non si sia già provveduto a cura del medesimo, in accordo con il Settore di appartenenza, a condividere con altri utenti i dati/files necessari all'attività lavorativa d'ufficio, il Responsabile/Dirigente del dipendente può richiedere formalmente al Settore Sistemi Informativi la "forzatura" della password dell'utente assente, comunicando la nuova password ad altro dipendente temporaneamente autorizzato ad accedere ai dati/files presenti sull'apparecchiatura del dipendente assente (stessa *user*).
   Tale richiesta, indirizzata al Settore Sistemi Informativi, comunicata al Dipendente incaricato della temporanea sostituzione, e, per conoscenza, al Dipendente temporaneamente assente, deve formalmente specificare:
   - la richiesta di accesso alle banche dati/files del P.C., compresi gli eventuali dati/files personali memorizzati ;
   - il nominativo del Dipendente/Incaricato assente;
   - il nominativo del Dipendente/temporaneamente incaricato sostituto.

   L'irreperibilità del dipendente assente non pregiudica, in ogni caso, l'accesso al p.c. da parte del Responsabile/Dirigente del dipendente medesimo e dei tecnici del SSI.
   Al rientro del dipendente assente, analoga richiesta formale dovrà richiedere l'intervento del Settore Sistemi Informativi per ri-forzare nuova password al suo precedente *user.*

9. In caso di cessazione del dipendente, occorre prontamente comunicare ogni variazione al Settore Sistemi Informativi per il conseguenti interventi: blocco account, eventuale salvataggio dati, recupero apparecchiatura ed eventuale ri-assegnazione ad altro Utente (altro Settore).

Art. 67
"Utilizzo della rete"

1. Per l'accesso alla Rete Comunale ciascun utente deve essere in possesso della specifica credenziale di autenticazione.

2. 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

ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.

3. Le cartelle utenti presenti nei server (computer o programmi di servizio ad altre componenti "client"-cliente) di sistema sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file (contenitore di informazione digitalizzata) 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, amministrazione e back up (copia di riserva di uno più files da parte del personale incaricato del Settore Sistemi Informativi).

4. Tutti i dischi o altre unità di memorizzazione locali (es. disco C interno al PC) non sono soggetti a salvataggio da parte del personale incaricato del Settore Sistemi Informativi. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo utente.

5. 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. 68
"Copie di sicurezza e misure di ripristino (Back-up e disaster recovery).

1. Il Dipendente è responsabile della periodica esecuzione delle necessarie copie di sicurezza di singoli file e/o cartelle di dati/documenti presenti sul proprio PersonalComputer, della modifica/aggiornamento e della sua corretta conservazione ed uso.

2. Le copie di sicurezza di file e/o dati memorizzati dagli applicativi gestionali in uso su archivi/dischi dei Server Centrali CED di Sala Macchine, sono invece di responsabilità del Settore Sistemi Informativi (incaricato del trattamento).

3. Per i file e/o dati presenti sulle memorie delle singole apparecchiature, il dipendente deve effettuare la copia di sicurezza almeno una volta alla settimana. La periodicità delle copie è valutata dal dipendente in base alla frequenza di aggiornamento/modifica dei dati medesimi e dall'eventuale danno originato dalla relativa perdita accidentale.

4. L'estensione/dimensione delle copie di sicurezza (singoli file e/o intere cartelle/sottocartelle) è valutata dal dipendente in base alle modalità tecniche di Back-Up possibili, in relazione ai dispositivi disponibili (chiavette USB, CD/DVD, dischi di rete e conseguenti spazi disponibili e tempi di copia).

5. Nell'ambito di una preventiva programmazione del fabbisogno, d'intesa con il Settore Sistemi Informativi, e delle risorse disponibili a bilancio, sui dischi di rete c/o Sala Macchine/CED sono anche disponibili, per ogni Settore, specifiche cartelle di settore, condivisibili tra utenti per scambiarsi dati/files e/o costituire, nel limite dello spazio a disposizione, piccoli archivi di Settore.
   La configurazione degli utenti e delle cartelle avviene d'intesa con il relativo Responsabile/Dirigente di riferimento.
   In particolare, eventuali esigenze di condivisione dati/files tra utenti di Settori diversi, se non diversamente risolvibili con condivisione in rete di cartelle del proprio hard disk (disco fisso/memoria di massa del personal computer) e/o scambio file tramite e-mail (posta elettronica), devono essere motivatamente concordate con il Settore Sistemi Informativi.

6. Il dipendente non cancellerà dal proprio personal computer dati/file eventualmente già copiati sui dischi di rete, sia per il maggior spazio disco disponibile sulla propria apparecchiatura, sia per i tempi di ripristino non immediati del server di rete/NAS in caso di guasto accidentale ed eviterà di lavorare esclusivamente e direttamente su cartelle del

server di rete/NAS, senza prevedere contemporaneamente anche ad una o più copie di file/dati anche sui propri personal computer di Settore.

7. Il dipendente effettuerà il Back-Up e le copie dei soli file/cartelle ritenuti veramente indispensabili alla continuità operativa del Settore di appartenenza e concorderà invece con il Settore Sistemi Informativi le modalità tecniche più idonee a costituire e conservare, a cura del Settore di appartenenza, archivi storici di maggiori dimensioni ed importanza.

Art. 69 Protezione antivirus

1. Il sistema informatico è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus od ogni altro software aggressivo *(malware)*.

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 incaricato del Settore Sistemi Informativi.

3. Ogni dispositivo per la memorizzazione dei dati di provenienza esterna dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente segnalato l'accaduto al personale incaricato del Settore Sistemi Informativi.

Art. 70 Utilizzo e conservazione dei supporti rimovibili

1. Tutti i supporti magnetici rimovibili (dischetti, CD e DVD, supporti USB, ecc.), contenenti dati personali, specie se sensibili, nonché qualunque informazioni aziendale, 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.

2. Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati personali, specie se sensibili, ciascun utente dovrà contattare il personale del Settore Sistemi Informativi e seguire le istruzioni da questo impartite.

3. In ogni caso, i supporti magnetici contenenti dati personali, specie se sensibili devono essere dagli utenti adeguatamente custoditi in armadi o cassetti chiusi.

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

5. Tutti i dati personali, specie se sensibili, riprodotti su supporti magnetici o su supporti cartacei devono essere trattati e custoditi con particolare cautela onde evitare che il loro contenuto possa essere accessibile. Non è pertanto consentito, per es., lasciare incustoditi presso le stampanti documenti cartacei, specie se contenenti dati sensibili, ed è necessario riporre e custodire i supporti magnetici in luoghi sicuri, quali, almeno, cassetti/armadi chiusi a chiave.

Art. 71 Utilizzo di personal computer portatili (notebook)

1. I personal computer portatili possono essere motivatamente assegnati quando la natura delle prestazioni e dell'incarico (esigenze di servizio) richiedano operatività in luoghi anche diversi dalla usuale sede di lavoro, ovvero in relazione a particolari forme di prestazione dell'attività lavorativa (ad esempio: telelavoro), ferma restando la verifica del miglior rapporto costo/prestazioni dei notebook stessi rispetto alle effettive esigenze operative.

2. L'utilizzo dei personal computer portatili segue le stesse regole previste per i personal computer fissi connessi in rete.

3. L'utente è responsabile del PC portatile assegnatogli e deve custodirlo con cura e diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro per evitare danni o sottrazioni. L'eventuale furto o smarrimento, previa formale denuncia alle Autorità competenti, deve essere tempestivamente comunicata al Settore Sistemi Informativi.

4. Per i personal computer portatili, particolare attenzione e cautela deve essere posta nella memorizzazione e custodia dei dati, nell'ottica di minimizzare il rischio di perdita o sottrazione indebita di dati rilevanti nella eventualità di furto o smarrimento.

Art. 72
"Utilizzo di Internet"

1. L'utilizzo di Internet deve essere limitato a scopi inerenti l'attività lavorativa.

2. E' consentito, per scopi personali, l'utilizzo di Internet durante la pausa pranzo o, per esigenze straordinarie ed urgenti per l'assolvimento di incombenze amministrative e burocratiche, purchè contenuto nei tempi strettamente necessari allo svolgimento delle transazioni stesse.

3. E' consentito l'accesso, solo tramite Internet a caselle webmail di posta elettronica personale.

4. L'amministrazione si riserva di applicare profili di navigazione personalizzati per gruppi di utenti o per settori, a seconda dell'attività professionale svolta.
   Attraverso tale "profilazione", saranno consentite le sole attività di accesso, navigazione, e, se necessario, registrazione a siti, scaricamento (download), ascolto e visione di file audio / video in modo personalizzato e correlato con la propria attività lavorativa.

5. Non è comunque consentito l'accesso, la navigazione e la registrazione a categorie di siti ritenuti non sicuri o non appropriati dall'amministrazione, individuate attraverso un apposito sistema di filtro e blocco della navigazione per l'accesso a tali categorie di siti (URL filtering).

6. Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, l'Amministrazione rende peraltro nota l'adozione di uno specifico sistema di blocco o filtro automatico che previene determinate operazioni quali l'upload caricamento di dati dall'utente verso un server remoto) o l'accesso a determinati siti inseriti in appositi elenchi (black list).

7. Tutte le attività che coinvolgono un transito di dati da e verso internet vengono registrate e custodite all'interno di un server dedicato (*Proxy Server*), formando automaticamente un registro cronologico delle operazioni effettuate ("*file di log*"), il cui accesso è consentito esclusivamente al personale incaricato (Amministratore di Sistema) del Settore Sistemi Informativi.
   Il controllo sui file di log non è continuativo ed i file stessi vengono conservati non oltre 3 mesi.

8. Periodicamente possono essere generati rapporti statistici aggregati nei quali non compare alcuna relazione utente-contenuto, ma vengono semplicemente elencati i siti maggiormente visitati, le destinazioni IP più richieste, gli utenti che hanno generato il maggior volume di traffico dati e l'utilizzo della banda internet per orari del giorno e per giorni della settimana.
   Nel caso si ravvisassero abusi e/o anomalie, l'Amministrazione attiva, nel rispetto della normativa sulla tutela e riservatezza dei dati personali, un sistema di verifiche graduale sull'utilizzo corretto di Internet, come meglio specificato al successivo art. 76.

9. E' fatto salvo un eventuale prolungamento dei tempi di conservazione dei dati, (comunque limitato al raggiungimento degli scopi perseguiti) giustificato da specifica, motivata e comprovata finalità oppure dall'obbligo di custodire e consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o di polizia giudiziaria, o,

infine, dall'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria.

Art. 73
"Gestione ed utilizzo della posta elettronica"

1. La casella di posta elettronica *individuale* (n.cognome@sestosg.net*)* viene assegnata d'ufficio agli Amministratori, al Segretario Generale, ai Dirigenti, ed ai dipendenti che, per le funzioni svolte, sono dotati di personal computer.

2. Per particolari forme di lavoro, non provviste di personal computer, qualora le funzioni svolte richiedano comunque l'uso della posta elettronica, la casella di posta elettronica individuale può essere assegnata solo su espressa richiesta del Responsabile/Dirigente di riferimento che individua anche, d'intesa con il Settore Sistemi Informativi, i personal computer da cui accedervi.

3. Eventuali caselle di posta elettronica condivise da più utenti (es.: serv_anagrafe@sestosg.net o assistenzaced@sestosg.net) vengono assegnate solo per motivate esigenze di servizio e solo su espressa richiesta del Responsabile/Dirigente di riferimento che, d'intesa con il Settore Sistemi Informativi, ne definisce nome ed utenti, individuando comunque un responsabile nella gestione della stessa.

4. Per una corretta gestione tecnico/economica dello spazio disco, sul server di posta dell'Ente, la dimensione delle caselle è commisurata a motivate esigenze lavorative.

5. La casella di posta elettronica assegnata è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
   La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.
   Il dipendente deve tenere una corretta gestione dell'account e relativa password a tutela della privacy ed usi impropri.

6. Solo per caselle individuali è comunque consentito, in via eccezionale, un utilizzo limitato delle stesse per scopi personali, secondo le norme dettate dal presente regolamento, prevalentemente durante la pausa pranzo o per improrogabili esigenze straordinarie e del tutto occasionali.

7. E' fatto divieto di utilizzare la casella di posta elettronica per:
   - trasmissione di dati sensibili e di tutti gli altri dati personali, nell'ambito della propria attività lavorativa, salvo nei casi previsti da espressa disposizione di legge e nell'osservanza delle disposizioni vigenti in materia di privacy;
   - partecipazione a dibattiti, forum, o mailing-list non attinenti la propria attività lavorativa o funzione svolta per l'Ente, salvo diversa ed esplicita autorizzazione.

8. Per una corretta gestione delle dimensioni delle caselle di posta elettronica e per non contribuire ad innescare inutili disservizi, costi di manutenzione e minacce alla sicurezza, non è consentito l'invio/ricezione di messaggi con allegati di dimensione superiori a 15Mb e con estensione uguali a .lnk, .bat, .exe, .scr e, in generale, file di tipo video/audio, non legati all'attività lavorativa, od eseguibili o di applicazioni.
   Il sistema di sicurezza e antivirus installato a protezione del server di posta elettronica non consente la ricezione e l'invio di messaggi di posta che contengono allegati con le caratteristiche sopra elencate. Eventuali particolari esigenze lavorative potranno essere segnalate al Settore Sistemi Informativi che individuerà la soluzione tecnica più appropriata.

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

10. La posta elettronica può essere configurata in due modi diversi:
    - POP: protocollo che ha il compito di permettere, mediante autenticazione, l'accesso ad un account di posta elettronica presente sul server del Comune per scaricare le e-mail del relativo account sul proprio dispositivo. I messaggi di posta elettronica, per essere letti, devono essere scaricati sul computer; di norma lo scarico dei messaggi avviene ogni 30 min.
    - IMAP: con il protocollo IMAP l'utente puo' avere a disposizione l'intero insieme dei propri messaggi da qualsiasi PC, Notebook o Smartphone ci si connetta perchè questi vengono mantenuti sul server.

    Resta comunque possibile, previa autenticazione con l'account e la password assegnata, anche l'accesso via web, direttamente al server - http://mailserver.sestosg.net, specie agli utenti sprovvisti di PC e/o al di fuori della rete comunale.

11. A garanzia del corretto funzionamento ed in considerazione delle specifiche caratteristiche tecniche della posta elettronica, in relazione anche alle effettive dimensioni allocate, ogni utente, con il supporto del Settore Sistemi Informativi, è responsabile della corretta tenuta della propria casella di posta, con particolare riferimento alla cancellazione, archiviazione e back-up dei propri messaggi, specie di tutti quelli, nel tempo, inviati e ricevuti, oltre le specifiche dimensioni configurate sul Server di Posta e, eventualmente, scaricati sui propri dispositivi.
    A garanzia della continuità di servizio il CED provvede, quotidianamente, al back-up dei soli messaggi presenti sulle cartelle del Server di Posta e, eventualmente, non ancora scaricati.

12. In caso di assenze dal lavoro programmate o non programmate, l'interessato deve provvedere, d'intesa con il Settore Sistemi Informativi, a configurare la propria casella di posta elettronica per l'invio di un messaggio di risposta automatica o, se necessario, per motivate esigenze di servizio, per il trasferimento/inoltro ad altra casella designata dei dati ritenuti rilevanti ed urgenti per lo svolgimento dell'attività lavorativa.

13. In caso di cessazione del rapporto di lavoro, l'indirizzo di posta elettronica individuale dell'interessato viene mantenuto attivo per un periodo di tempo pari a quattro settimane. Al termine, viene definitivamente cessato sia l'indirizzo stesso che ogni eventuale messaggio. ancora presente.

Art. 74
"Osservanza delle disposizioni in materia di privacy"

1. L'utente ha l'obbligo di custodire e controllare i dati personali trattati con strumenti elettronici nell'osservanza delle disposizioni del Codice in materia di protezione dei dati personali nonché delle istruzioni operative per l'adozione delle misure di sicurezza nell'utilizzo del sistema informativo comunale, allegate alla propria lettera d'incarico trattamento dati personali.

Art. 75
"Accesso ai dati trattati dall'utente"

1. Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.) o per finalità di controllo e programmazione dei costi (ad esempio, verifica costi di connessione ad internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà dell'Amministrazione, per il tramite del personale incaricato del Settore Sistemi Informativi

(o addetti alla manutenzione incaricati), accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici ed ai documenti ivi contenuti, degli apparati di servizio dati in dotazione agli utenti.

Art. 76
"Sistemi di controllo graduali"

1. L'Amministrazione si riserva di effettuare controlli sul corretto utilizzo degli strumenti informatici e telematici nel rispetto delle normative vigenti e del presente regolamento.

2. Per esigenze organizzative, produttive e di sicurezza l'Amministrazione, mediante il personale incaricato del Settore Sistemi Informativi, può avvalersi di strumenti che consentono un controllo a distanza di tipo generalizzato, indiretto e anonimo, relativo all'intera struttura amministrativa, ad aree, settori o gruppi di utenti.

3. In caso di anomalie, l'Amministrazione procede preliminarmente all'invio di un avviso generalizzato relativo all'uso improprio riscontrato, con l'invito agli interessati ad attenersi scrupolosamente al presente regolamento, riservandosi, successivamente, la facoltà di svolgere ulteriori controlli, su base individuale, solo in caso di successive ulteriori anomalie.

4. In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

Art. 77
"Sanzioni"

1. E' fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente regolamento.

2. In caso di abuso, a seconda della gravità del medesimo, e fatte salve ulteriori conseguenze di natura penale, civile ed amministrativa, possono essere comminate le sanzioni disciplinari previste dalla normativa vigente in materia e dai contratti di lavoro, nonché delle eventuali azioni risarcitorie.

Art. 78
"Entrata in vigore, aggiornamento e revisione, Norma finale."

1. Il presente regolamento entrerà in vigore dalla data di pubblicazione sul sito istituzionale.

2. Il presente regolamento viene pubblicato sul sito istituzionale del Comune e portato a conoscenza di ciascun dipendente.

3. Per tutto quanto non espressamente disciplinato dal presente regolamento, si rimanda, in quanto compatibili, alle norme di legge, dello Statuto Comunale, dei regolamenti e dei C.C.N.L. dei dirigenti e del personale dipendente degli Enti Locali.