DISCIPLINARE PER L'UTILIZZO DELLA DOTAZIONE INFORMATICA DEL COMUNE DI SANREMO

Revisione approvata con Deliberazione della Giunta Comunale n. 315 del 21/12/2018
Adottato con Deliberazione della Giunta Comunale n.177 del 31/08/2016

CAPO I

PREMESSA

Negli ultimi anni l'organizzazione del lavoro è stata sottoposta ad un imponente processo di informatizzazione e, in tale contesto, i servizi di rete, tra cui posta elettronica e Internet, sono diventati strumenti quotidiani indispensabili per l'esercizio dell'attività lavorativa.

Tuttavia l'utilizzo di tali strumenti in maniera non corretta, anche a seguito di comportamenti inconsapevoli, può essere causa di gravi minacce e problemi per la sicurezza del sistema e delle informazioni in esso contenute.

A ciò aggiungasi che le informazioni trattate nell'ambito dell'attività lavorativa possono riguardare la sfera personale e la vita privata dei lavoratori e di terzi per cui le attività di monitoraggio cui possono essere sottoposte le risorse informatiche messe a disposizione sia del personale dell'Ente che dei fornitori esterni dovranno sempre ispirarsi al rispetto della normativa sulla tutela della riservatezza dei dati personali nonché ai principi di diligenza e correttezza.

ART. 1 - FINALITÀ

1. Il presente regolamento è diretto a definire le modalità di accesso ed utilizzo degli strumenti informatici, di internet e della posta elettronica, nell'ambito dello svolgimento delle proprie mansioni e compiti, ai fini di un corretto utilizzo degli strumenti stessi da parte degli amministratori, dipendenti e collaboratori del Comune di Sanremo.

2. L'Amministrazione promuove ogni opportuna misura, organizzativa e tecnologica, volta a prevenire il rischio di utilizzi impropri delle strumentazioni e delle banche dati di proprietà del Comune e disciplina le modalità con cui effettuerà i relativi controlli.

3. L'Amministrazione promuove anche lo sviluppo e la promozione culturale dei dipendenti a contatto con tali strutture e lo sviluppo e potenziamento delle stesse.

4. Premesso che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza (Decreto del Presidente della Repubblica del 16 Aprire 2013 n. 62), il presente regolamento è diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

5. Le prescrizioni di seguito previste integrano le specifiche istruzioni già fornite a tutti gli autorizzati in attuazione del Regolamento UE n. 2016/679 (GDPR) e del decreto legislativo 30 giugno 2003 n. 196, aggiornato al decerto legislativo 10 Agosto 2018 n. 101, comprese le misure di sicurezza (tecniche e organizzative) adeguate ed eventuali altri documenti contenenti eventuali ulteriori misure specifiche.

6. Il presente regolamento integra il Codice di Comportamento dei Dipendenti delle Pubbliche Amministrazioni per quanto riguarda l'utilizzo degli Strumenti Informatici, ai sensi dell'Art. 54 del Decreto Legislativo n. 165 del 30 Marzo 2001 e s.m.i.

7. Per quanto non espressamente previsto dal presente atto, si rinvia alle disposizioni generali vigenti in materia, con particolare riferimento alle Linee Guida del Garante per Posta Elettronica e Internet (Delib. Garante Privacy n. 13 del 1° marzo 2007), ed alla Direttiva della Presidenza del Consiglio dei Ministri - Dipartimento della Funzione Pubblica- n. 2/2009.

ART. 2 - AMBITO DI APPLICAZIONE

1. La rete del Comune di Sanremo è 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 ed in generale tutti i documenti prodotti tramite l'utilizzo dei suddetti apparati.

2. Il presente disciplinare si applica a tutti gli utenti che a diverso titolo sono autorizzati ad accedere alla rete comunale. Per utenti si intendono gli amministratori, i dirigenti, i dipendenti a tempo indeterminato e determinato ed i collaboratori impiegati a diverso titolo presso l'amministrazione, compreso il personale fornito da terze parti e gli utenti esterni. Per utenti esterni si intendono tutti i soggetti che usufruiscono dei sistemi informativi per erogare un servizio pubblico (ad esempio, consultazioni anagrafiche).

3. Il presente regolamento per l'utilizzo degli strumenti informatici e modalità di controllo è pubblicato sul sito internet nella sezione Amministrazione Trasparente assieme al codice di comportamento di cui costituisce parte integrante.

ART. 3 – PRINCIPI GENERALI

1. Il Comune di Sanremo promuove l'utilizzo degli strumenti informatici, di internet e della posta elettronica quali mezzi utili a perseguire con efficacia ed efficienza le proprie finalità istituzionali, in accordo con le linee guida e i principi delineati dalla normativa vigente.

2. Ogni utente è responsabile, civilmente e penalmente, del corretto uso delle risorse informatiche, con particolare riferimento ai servizi, ai programmi a cui ha accesso e ai 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 un danno, anche di immagine, all'Ente.

3. Il lavoratore deve custodire ed utilizzare gli strumenti informatici, internet, la posta elettronica in modo appropriato e diligente ed è responsabile della propria postazione di lavoro.

4. I documenti prodotti dagli utenti e memorizzati nell'hardware di proprietà del Comune, sono da considerare a pieno titolo nella disponibilità dell'Ente.

5. Le disposizioni di cui al presente regolamento sono assolutamente obbligatorie e inderogabili, salva espressa autorizzazione. La loro violazione comporterà per il lavoratore sanzioni disciplinari.

6. Ogni utente/autorizzato viene adeguatamente istruito – ed eventualmente aggiornato - sulle modalità e sulle regole di utilizzo degli strumenti informatici, mediante consegna di regolamento sull'utilizzo degli strumenti informatici, attraverso formazione in affiancamento e, in casi particolati, a scelta del Titolare, attraverso formazione diretta o a distanza (anche tramite tutorial). Qualora l'autorizzato ritenesse inadeguate le istruzioni ricevute, potrà senza indugio farlo presente, così da ricevere le integrazioni necessarie.

CAPO II

ART. 4 – CRITERI GENERALI

1. Tutto l'hardware ed il software in dotazione agli uffici deve essere acquisito in accordo con le specifiche tecniche fornite dal Servizio Sistemi Informativi, competente per la materia.
   L'utilizzo delle stampanti e dei materiali di consumo in genere (carta, inchiostro, toner, supporti magnetici, supporti digitali) è riservato esclusivamente per lo svolgimento di compiti di natura strettamente istituzionale. Devono essere evitati in ogni modo sprechi dei suddetti materiali o utilizzi eccessivi.

2. Laddove materialmente possibile e conformemente alla legislazione vigente, gli utenti devono utilizzare prevalentemente le stampanti compartimentali (o di piano), le stampanti di tipo personale sono riservate esclusivamente ad utilizzo sporadico/di emergenza: i Dirigenti e gli Amministratori si impegnano ad eliminare, ove possibile, le stampanti e/o gli scanner personali in favore di dispositivi compartimentali (o di piano), che permettono un risparmio nei costi di gestione.
   Tutte le stampanti multifunzione di rete, i plotter e stampanti laser a colori messi a disposizione dal sistema informativo dell'Ente, indipendentemente dalla collocazione negli uffici e geografica, sono a disposizione di tutti gli Utenti che, per esigenze di servizio, debbano utilizzarli.

3. Ogni possessore di hardware e software è tenuto all'uso appropriato e alla sua diligente conservazione. E' inoltre tenuto all'autonoma conservazione della relativa documentazione, della licenza d'uso, dei supporti magneto-ottici (dischi, DVD, CD, nastri magnetici, ecc.) e di qualsiasi altro materiale consegnato contestualmente all'hardware o al software. Tale materiale potrà essere richiesto per esigenze di servizio quali, ad esempio, il ripristino del funzionamento dell'hardware o del software.

4. Tutti gli utenti e comunque autorizzati sono tenuti all»assoluta segretezza in merito ai dati trattati, alle informazioni di cui in ogni modo sono venuti a conoscenza, nonchè delle procedure apprese/utilizzate.

ART. 5 – MODALITÀ DI UTILIZZO DEGLI STRUMENTI INFORMATICI

Durante l'espletamento della propria attività lavorativa, i dipendenti devono attenersi alle seguenti istruzioni e raccomandazioni:

1. Per evitare il grave pericolo di introdurre virus informatici nei sistemi comunali, devono essere utilizzati esclusivamente programmi distribuiti dall'Ente; in particolare è vietato scaricare files e software anche gratuiti, prelevati da siti internet, se non su espressa autorizzazione del Dirigente o Responsabile di Settore competente, di concerto con il Servizio Sistemi Informativi. Fermi restando i precedenti divieti, l'utente è abilitato ad effettuare autonomamente gli aggiornamenti gratuiti dei software già installati sul PC.

2. Non è consentito modificare la configurazione impostata sul proprio PC e installare periferiche (hard-disk, DVD, fotocamere, apparati multimediali, periferiche USB, ecc …) esterne agli strumenti in dotazione se non per esigenze di servizio, autorizzate dal Dirigente o dal Responsabile di Settore, di concerto con il Servizio Sistemi Informativi.

3. Al fine di evitare di introdurre virus, si raccomanda di non copiare files di provenienza incerta da supporti quali pen drive, Cd-ROM, DVD, ecc.. per finalità non attinenti alla propria prestazione lavorativa.

4. Gli applicativi gestionali (Gestione Protocollo, Atti Amministrativi, Anagrafe, ecc …) sono destinati alla gestione di informazioni il cui utilizzo deve essere compatibile con la normativa vigente relativa alla privacy (vedi dlgs 196/2003 e successive modificazioni).

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

6. E' vietata l'installazione non autorizzata di modem che sfruttino il sistema di comunicazione telefonico per l'accesso a internet o a banche dati esterne.

7. Non è consentito agli utenti duplicare e/o cedere programmi e altro materiale informatico, se non nelle forme e per gli scopi di servizio per i quali sono stati assegnati e nel rispetto della legislazione vigente.

8. L'eventuale malfunzionamento o danneggiamento del personal computer deve essere tempestivamente comunicato al Servizio Sistemi Informativi tramite richiesta di assistenza HelpDesk.

9. I sistemisti ed i tecnici che hanno in gestione e seguono la manutenzione dei componenti del sistema informatico comunale possono procedere, dandone prima preavviso, alla rimozione dei files o applicazioni che riterranno essere pericolosi per la sicurezza sia sui singoli personal computer, sia sulle unità di rete, anche senza preavviso in casi di elevata emergenza.

10. I sistemisti ed i tecnici Servizio Sistemi Informativi incaricati della gestione e della manutenzione dei componenti del sistema informatico comunale possono, in qualsiasi momento, accedere al personal computer (anche con strumenti di supporto, assistenza e diagnostica remota) per manutenzione preventiva e correttiva, previa autorizzazione dell'utente o richiesta di assistenza tramite HelpDesk.

11. Ogni dipendente che dovrà per qualsiasi motivo lasciare incustodita la propria postazione di lavoro sarà tenuto a bloccarla (ad esempio, mediante l'utilizzo di CTRL+ALT+CANC → "Blocca Computer", oppure salvaschermo dotato di password o eventuale estrazione e custodia dell'hardware di autenticazione e degli altri supporti removibili) o spegnere fisicamente il computer.

ART. 6 – GESTIONE DEGLI ACCESSI ALLA RETE COMUNALE

1. Il Servizio Sistemi Informativi, in funzione delle esigenze operative comunicate dal Dirigente del Servizio interessato o dal Servizio Personale, assegna, sospende e revoca le credenziali di autenticazione e le autorizzazioni all'accesso ai servizi hardware, software e di posta elettronica erogati dal sistema informativo attraverso le reti Intranet / Internet.
   Le autorizzazioni di accesso al sistema informativo sono assegnate in funzione delle esigenze operative comunicate dalla Dirigenza e della collocazione dell'Utente nell'organigramma.

2. In caso di cessazione del rapporto di lavoro, l'account individuale del dipendente verrà dismesso secondo quanto previsto dal dlgs 196/2003 e s.m.i.

3. Le ditte esterne ospitate nei locali dell'Ente così come il personale esterno incaricato dall'Ente (es. consulenti, stagisti, personale interinale) possono, previa autorizzazione, usufruire del sistema informativo Comunale: il personale esterno incaricato e autorizzato dall'Ente è a tutti gli effetti un Utente del sistema informativo comunale ed è soggetto alle presenti norme operative.
   Le richieste di autorizzazione all'accesso devono essere trasmesse dal Dirigente del Servizio interessato al competente Responsabile del Servizio Sistemi Informativi.
   L'accesso alle aree di servizio/ufficio deve essere attentamente valutato e chiaramente indicato nella richiesta: di norma, le credenziali per il personale esterno sono a tempo e quindi al momento del rilascio deve essere chiaramente indicata la data di scadenza (fine rapporto).

ART. 7 – GESTIONE DELLE CREDENZIALI DELL'UTENTE

1. Si distinguono le credenziali di accesso alla rete e quelle di accesso ai programmi autorizzati, ciascuno con una specifica password, in particolare:
   - password di rete, per l'avvio e l'utilizzo del sistema operativo e di tutte le risorse di rete compresa la posta elettronica;
   - password per l'accesso a particolari programmi e applicativi, ivi compresa la intranet

2. Le credenziali di autenticazione dell'Utente sono costituite dalla coppia <User-id, Password>, vengono rilasciate secondo gli standard in uso nell'Ente e sono riconducibili alla seguente forma:
   - user-id
   - password alfanumerica inizializzata dal Servizio Sistemi Informativi ed obbligatoriamente cambiata al primo utilizzo da parte dell'Utente.

3. La coppia <User-id, Password> identifica univocamente l'Utente;.

4. Per l'accesso alla Posta Elettronica è necessario utilizzare il proprio indirizzo e-mail e la Password di rete così come definita al punto 2. L'Articolo 13 disciplina nel dettaglio l'utilizzo della Posta Elettronica.

5. Non è consentita l'attivazione della password di accensione (bios) del personal computer;

6. L'Utente è informato del fatto che la conoscenza di entrambe le parti delle credenziali da parte di terzi consentirebbe a questi ultimi l'utilizzo del sistema informativo e dei servizi erogati attraverso di esso. L'Utente si impegna a non rivelare ad alcuno le proprie credenziali di autenticazione per l'accesso al sistema informativo: ogni individuo è responsabile civilmente e penalmente della custodia e della segretezza delle proprie credenziali (v. dlgs 196/2003 e s.m.i.).

7. L'Utente è il solo ed unico responsabile della conservazione e della riservatezza della propria password e, conseguentemente, rimane il solo ed unico responsabile per tutti gli usi ad essa connessi o correlati, (ivi compresi danni e conseguenze pregiudizievoli arrecati all'Ente e/o a terzi) siano dal medesimo utente autorizzati ovvero non autorizzati.

8. L'Utente si impegna a comunicare quanto prima al Servizio Sistemi Informativi l'eventuale furto, smarrimento o perdita delle credenziali. In particolare, in caso di furto, l'Utente si impegna a modificare tempestivamente la password utilizzando le procedure automatiche a sua disposizione. In ogni caso, resta inteso che l'Utente sarà responsabile delle conseguenze derivanti dal furto, dalla perdita o dallo smarrimento delle sue credenziali.

9. Qualora sussista il dubbio di violazione della segretezza, l'utente dovrà provvedere al cambiamento della password.

10. Al primo accesso al sistema l'utente è obbligato a cambiare la password assegnata di default ed a porre in essere una gestione sicura della stessa nel rispetto dei seguenti requisiti:
    - la password deve essere diversa dallo User-ID;
    - deve avere lunghezza e caratteristiche tali da non essere facilmente identificata e/o deve essere conforme alle indicazioni date dalla procedura di impostazione password (v. dlgs 196/2003 e s.m.i.)
    - deve essere modificata periodicamente ai sensi della normativa in vigore (v. dlgs 196/2003 e s.m.i.) o secondo la procedura di modifica proposta automaticamente;
    - è fatto divieto all'utente di utilizzare password banali, ovvie, facilmente memorizzabili o agevolmente riconducibili all'utente; la password non deve essere costituita da predefinite sequenze alfanumeriche, né contenere riferimenti scontati o facilmente deducibili (nome del

mese corrente, sequenze con numeri progressivi, etc.) o riferimenti a carattere personale (date, numeri di telefono, nomi di persona, etc.)
- in Appendice sono riportate alcune indicazioni utili circa la scelta della Password

11. Si rende noto che nei casi in cui é indispensabile o indifferibile accedere ai dati trattati dall'utente ed agli strumenti informatici in dotazione allo stesso, sia per le esigenze organizzative e di servizio, sia per la sicurezza ed operatività dello stesso sistema informatico, il Servizio Sistemi Informativi del Comune potrà accedere agli strumenti elettronici personali, mediante l'intervento del personale appositamente incaricato ad operare, dietro richiesta del Responsabile al Trattamento dei dati. La stessa facoltà, sempre ai fini di garantire la salvaguardia e la sicurezza del sistema informatico e per ulteriori motivi tecnici e manutentivi, si applica anche in caso di assenza prolungata o impedimento dell'utente.

ART. 8 – PROPRIETÀ INTELLETTUALE E LICENZE

1. Tutto il software in uso nel sistema informativo Comunale in cui sia prevista una licenza d'uso deve essere ottenuto seguendo le procedure di acquisizione definite dai regolamenti interni e deve essere registrato a nome del Comune di Sanremo.

2. Tutto il software che non richieda una licenza d'uso a titolo oneroso, quale il software a sorgente aperto (open source) o il software distribuito con licenza d'uso di tipo freeware o shareware, deve essere selezionato e reso disponibile agli utenti dal Servizio Sistemi Informativi, competente per la materia.

3. Non è possibile installare, duplicare o utilizzare software acquisiti al di fuori di quanto consentito dagli accordi di licenza.

4. Tutti gli utenti sono tenuti al rispetto delle leggi in materia di tutela della proprietà intellettuale (copyright) sia per quanto riguarda il software che per quanto riguarda files multimediali.

ART. 9 – POSTAZIONE DI LAVORO

1. La configurazione base dell'hardware e l'installazione del software nelle postazioni di lavoro e negli apparati di rete di proprietà dell'Ente è predisposta dal personale del Servizio Sistemi Informativi o, previo accordo, da personale interno / esterno incaricato; l'Utente è tenuto a non modificare la configurazione base hardware e software della postazione di lavoro assegnata e degli apparati di rete messi a disposizione.

2. L'installazione del software di qualsiasi specie, dotato o meno di licenza d'uso a titolo oneroso, deve essere effettuata solo dal personale del Servizio Sistemi Informativi o da personale interno/esterno incaricato.

3. Ad ogni utente può essere assegnata apposita area di lavoro dedicata e/o una cartella condivisa su server/storage di dominio per la memorizzazione di dati e programmi accessibili ad un gruppo di utenti preventivamente autorizzati.
   L'utente è tenuto ad utilizzare le unità di rete per la condivisione di informazioni strettamente professionali; non può pertanto collocare, anche temporaneamente, in queste aree qualsiasi file che non sia attinente allo svolgimento dell'attività lavorativa. L'utente è tenuto, altresì, alla periodica (almeno ogni 6 mesi) pulizia di tutti gli spazi assegnati, con cancellazione dei files obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati al fine di evitare, salvo casi eccezionali, un'archiviazione superflua. A tale riguardo è possibile chiedere supporto al Servizio Sistemi Informativi (art. 15 – Assistenza – Procedure operative).

4. Il Servizio Sistemi Informativi provvede al salvataggio/backup delle basi dati e dei documenti presenti sui server del Comune di Sanremo.

5. L'utente è tenuto a conservare tutti i dati di lavoro nelle cartelle di rete, al fine di favorire la sicurezza dei dati, con la consapevolezza che tutti i dati contenuti nel computer locale sono maggiormente soggetti a perdita in caso di guasto del sistema. Il salvataggio e la salvaguardia dei dati presenti sul disco locale della postazione di lavoro sono ad esclusiva cura dell'utente.

6. Il Personal computer deve essere spento al termine di ogni turno giornaliero di lavoro, prima di lasciare gli uffici, e comunque deve essere protetto nelle pause durante l'orario di lavoro. Pertanto, ogni qualvolta il dipendente si allontani o si assenti dalla postazione di lavoro è tenuto a chiudere la sessione (Ctrl+Alt+Canc quindi "Blocca Computer"), oppure a rendere inaccessibile a terzi (ad esempio mediante l'utilizzo del salvaschermo dotato di password) la propria postazione di lavoro. E'

evidente che 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.

7. Tutti i supporti magnetici riutilizzabili (cd, dischetti, cassette e cartucce) contenenti dati personali, sia comuni che sensibili, devono essere trattati con particolare cautela. In alcuni casi, infatti, è possibile recuperare i dati memorizzati anche dopo la loro cancellazione. Per questo motivo il supporto, al termine dell'utilizzo, deve essere formattato prima di essere riutilizzato, oppure distrutto. L'operatore avrà cura di effettuare la stampa di documenti contenenti dati personali solo se strettamente necessaria provvedendo a ritirarli immediatamente dai vassoi delle stampanti condivise. Si dovrà limitare per quanto possibile, di dislocare stampanti e fax in aree accessibili a soggetti non abilitati al trattamento e non presidiate (per esempio: corridoi aperti al pubblico, sale d'attesa, ecc.).

8. Si possono effettuare copie di dati su supporti rimovibili (es. dischetti CD, DVD, chiavi usb) solo se autorizzati da parte del proprio Dirigente. Qualora sulle copie venissero trasferiti dati personali, gli stessi vanno utilizzati con le modalità previste dalla legge, e secondo il principio di necessità. Al termine del trattamento sarà cura del dipendente distruggere o rendere inutilizzabili i supporti rimovibili eventualmente utilizzati. I supporti rimovibili contenenti dati sensibili o giudiziari, se non utilizzati, devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri dipendenti, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e in alcun modo ricostruibili.

ART. 10 – PROTEZIONE DA MALWARE

1. Al fine di proteggere l'integrità del sistema informativo, il Comune di Sanremo si è dotato di:
   - apparati di sicurezza perimetrale che possono limitare la visibilità di siti web o servizi esterni e prevedere l'analisi del traffico da/verso Internet;
   - Sistema Antivirus centralizzato che protegge tutte le macchine in uso presso i vari Servizi ed Uffici;
   - Sistema anti-spam per l'analisi della posta elettronica.

2. L'antivirus è installato su ogni postazione di lavoro a cura del Servizio Sistemi Informativi. L'aggiornamento avviene in maniera automatica. Nel caso che il software antivirus rilevi la presenza di un virus che non è riuscito a ripulire, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer e segnalare l'accaduto al personale incaricato del Servizio Sistemi Informativi. Stessa cosa qualora noti comportamenti anomali quali esecuzione automatica di programmi, alterazione di file etc.

3. L'utente è tenuto ad osservare tutte le prescrizioni fornite dal Servizio Sistemi Informativi al fine di evitare infezioni e installazione di software malevolo, in particolare:
   - non utilizzare supporti removibili (per es.: chiavette/dischi esterni USB) senza autorizzazione del Dirigente e previa analisi degli stessi da parte del Servizio Sistemi Informativi;

   - non aprire allegati o visitare link contenuti in e-mail di dubbia provenienza; nel caso si abbiano dubbi in merito contattare preventivamente il Servizio Sistemi Informativi.

ART. 11 – UTILIZZO DI HARDWARE E SOFTWARE DI PROPRIETÀ PERSONALE

1. Al fine di proteggere l'integrità del sistema informativo, l'Utente non può connettere postazioni di lavoro o apparati personali alle reti LAN, Wireless, Intranet dell'Ente.

2. Il personale esterno incaricato può connettersi alle reti dell'Ente, per tutta la durata dell'incarico e con hardware di proprietà personale, previa richiesta al Servizio Sistemi Informativi. L'hardware sarà connesso alla rete e configurato a cura del Servizio CED o di personale interno/esterno incaricato dal Servizio stesso. Nel caso in cui l'hardware di proprietà personale non sia dotato di un software antivirus regolarmente aggiornato, sarà negato l'accesso alla rete.

3. Al fine di proteggere l'integrità del sistema informativo comunale, l'Utente non può utilizzare software di proprietà personale. Tutto ciò comprende anche le applicazioni regolarmente acquistate e registrate a titolo personale dall'Utente, i programmi shareware e/o freeware non resi disponibili dal Servizio Sistemi Informativi, il software scaricato da Internet o proveniente da supporti magneto-ottici allegati a riviste e/o giornali o altro software ottenuto o posseduto a qualsiasi titolo.

4. E' vietato l'uso di dispositivi di memorizzazione removibili scrivibili personali. Gli utenti che necessitino, per ragioni attinenti allo svolgimento dell'attività lavorativa, di utilizzare supporti di memorizzazione removibili devono farne richiesta all'Amministrazione attraverso il proprio Responsabile che dovrà sempre indicare una persona responsabile dell'utilizzo dei dispositivi assegnati. In caso di utilizzo di dispositivi di memorizzazione rimovibili assegnati dall'Amministrazione, l'utente dovrà comunque provvedere alla custodia e all'uso dei medesimi adottando tutti gli accorgimenti necessari per evitare accessi non autorizzati e/o trattamenti non consentiti dei dati in essi contenuti. Egli dovrà in particolare distruggere i dati sul dispositivo al termine del loro utilizzo per evitare la creazione di copie non controllate.

CAPO III

ART. 12 – UTILIZZO DELLA POSTA ELETTRONICA

La gestione delle caselle e-mail avviene in modo centralizzato su server; il servizio è erogato secondo i massimi standard di sicurezza garantendo elevata disponibilità e possibilità di essere fruito sia dalla rete Comunale che dall'esterno tramite PC, smartphone, tablet etc.

1. La casella di posta elettronica assegnata è uno strumento di lavoro ed il suo utilizzo è consentito solo per finalità connesse allo svolgimento della propria attività lavorativa e per le comunicazioni di servizio di carattere sindacale; è fatto divieto di associare alla casella assegnata qualsivoglia informazione di carattere personale che non sia pertinente alle attività dell'Ente. Le persone assegnatarie sono responsabili del corretto utilizzo della stessa.

2. L'assegnazione dell'indirizzo di posta elettronica può avvenire contestualmente all'assegnazione delle credenziali di autenticazione dell'Utente o secondo necessità.

3. L'accesso al servizio di posta elettronica da parte di un Utente avviene mediante le credenziali di autenticazione (user-id e password) di accesso al sistema informativo, rilasciate secondo le modalità individuate all'Articolo 7, l'Utente è informato del fatto che la conoscenza delle credenziali di autenticazione da parte di terzi consentirebbe a questi ultimi l'utilizzo del servizio di posta elettronica in nome dell'Utente medesimo e l'accesso alla sua corrispondenza di posta elettronica. L'Articolo 7 definisce le modalità per la corretta conservazione, responsabilità ed uso delle credenziali.

4. L'invio e la ricezione di messaggi di posta elettronica è consentito per lo scambio di comunicazioni e documenti utili all'esercizio della propria attività lavorativa; tale modalità va utilizzata ordinariamente; qualora si necessiti di attestazione ufficiale è invece necessario utilizzare la PEC (la Posta elettronica certificata è un tipo particolare di posta elettronica, disciplinata dalla legge italiana, che permette di dare a un messaggio di posta elettronica lo stesso valore legale di una raccomandata con avviso di ricevimento tradizionale garantendo così il non ripudio)

5. Nell'utilizzo della posta elettronica dell'Ente l'utente è tenuto ad osservare alcune norme di comportamento:
   - leggere sistematicamente i messaggi di posta elettronica e di PEC se di sua competenza;
   - alimentare correttamente il flusso documentale dell'Ente sia ai fini della trattazione sia ai fini dell' idonea conservazione;
   - i messaggi devono essere preferibilmente di solo testo, evitando ove possibile ogni formattazione e inserzione di immagini / motivi decorativi;
   - è buona norma inviare messaggi sintetici che descrivano in modo chiaro la questione;
   - indicare sempre chiaramente l'oggetto, in modo tale che il destinatario possa immediatamente individuare l'argomento del messaggio ricevuto, facilitandone la successiva ricerca per parole chiave;
   - inviare messaggi di posta elettronica a indirizzi plurimi numerosi (decine di destinatari) solo in casi motivati da esigenze di servizio;
   - rispettare le regole e le indicazioni operative che gli verranno fornite dal Servizio Sistemi Informativi; non violare il segreto della corrispondenza personale e il diritto alla riservatezza;
   - non immettere in rete informazioni che possano presentare forme o contenuti di carattere pornografico, osceno, blasfemo, razzista, diffamatorio o offensivo
   - non è consentita la trasmissione, a mezzo posta elettronica o PEC, di dati sensibili se non precedentemente criptati;
   - non è consentita la trasmissione e ricezione, a mezzo posta elettronica o PEC, di mail di carattere personale o, comunque, non attinenti ai compiti di ufficio;

- non è consentito inviare tramite posta elettronica messaggi pubblicitari e/o promozionali o comunicazioni ad altri utenti e/o gruppi di discussione senza che sia stato richiesto ed ottenuto il relativo consenso ovvero senza che tale invio sia stato sollecitato in modo esplicito;
- non è consentita l'iscrizione a mailing-list non legate ad esigenze professionali;
- non è consentito l'invio di lettere a catena (es. catena di S. Antonio); ciò include lettere per nobili cause vere o presunte;
- non è consentito trasmettere materiale e/o messaggi che incoraggino terzi a mettere in atto una condotta illecita e/o criminosa passibile di responsabilità penale o civile;
- non è consentito l'utilizzo di programmi di sicurezza e/o crittografia non previsti esplicitamente dalle procedure di sicurezza messe in atto dal Servizio Sistemi Informativi.

6. In caso di assenza prolungata programmata del dipendente è raccomandata l'attivazione del sistema di risposta automatica ai messaggi di posta elettronica ricevuta indicando, nel messaggio di accompagnamento, le coordinate di un collega o della struttura di riferimento che può essere contattata e/o altre modalità utili di contatto della struttura cui il lavoratore è assegnato

ART. 13 – UTILIZZO DI INDIRIZZI DI POSTA ISTITUZIONALI GENERICI (LISTE DI DISTRIBUZIONE)

1. L'assegnazione di un indirizzo di posta elettronica generico assegnato ad un servizio/ufficio/settore (ad esempio ufficio.nomedelufficio@comunedisanremo.it) può essere richiesto esclusivamente dalla Dirigenza dell'Ente la quale darà indicazioni sugli utenti che dovranno essere abilitati dal Servizio Sistemi Informativi ad utilizzare tale tipologia di indirizzo.

ART. 14 – UTILIZZO DI INTERNET

1. Gli utenti sono tenuti ad utilizzare il collegamento ad Internet unicamente per motivi legati ai propri doveri di ufficio. Sono esplicitamente vietati/e:
   - l'uso e la navigazione su siti web non legati ad esigenze esclusivamente di tipo lavorativo ed informativo ed in particolare che possano presentare forme o contenuti di carattere pornografico, osceno, blasfemo, razzista, diffamatorio o offensivo;
   - il download o la condivisione via Internet/Extranet/Intranet di file, anche di tipo audio/video o immagini, non legati alle attività professionali;
   - lo svolgimento di qualsiasi attività intesa ad eludere o ingannare i sistemi di controllo di accesso e/o sicurezza di qualsiasi server interno o pubblico;
   - l'uso di meccanismi o strumenti di qualsiasi natura atti ad eludere gli schemi di protezione da copia abusiva del software, a rivelare password, ad identificare eventuali vulnerabilità della sicurezza dei vari sistemi, a decrittare file crittografati o a compromettere la sicurezza della rete in qualsiasi modo;
   - al fine di non creare situazioni di sovraccarico della rete dati, non è permesso, per motivi non professionali, l'utilizzo sistematico della rete per la visualizzazione o l'ascolto di contenuto multimediale;
   - la partecipazione a forum, chat line, bacheche elettroniche e social network (ad esempio Facebook e similari) è permessa unicamente per motivi istituzionali o professionali
   - è vietata la consultazione delle banche dati a pagamento per finalità non pertinenti ai propri doveri d'ufficio, pur essendo autorizzati all'accesso;
   - non è consentito scambiare materiale protetto dalla normativa vigente in tema di tutela del diritto d'autore e utilizzare sistemi di scambio dati/informazioni con tecnologie "peer to peer" (da utente a utente).
   - l'accesso a siti e l'utilizzo di strumenti di social networking
   - l'utilizzo di strumenti di file sharing di qualsiasi natura, esclusi quelli eventualmente resi disponibili dal Servizio Sistemi Informativi

2. Durante l'orario di lavoro, come previsto dalla direttiva 02/09 Brunetta, agli utenti è consentito "assolvere incombenze amministrative e burocratiche senza allontanarsi dal luogo di lavoro (ad esempio, per effettuare adempimenti on line nei confronti di pubbliche amministrazioni e di concessionari di servizi pubblici, ovvero per tenere rapporti con istituti bancari e assicurativi)." Tale attività deve essere contenuta in tempi strettamente necessari allo svolgimento delle transazioni. Non è consentito ad esempio effettuare trading on line con istituti di credito.

3. L'accesso alla rete Internet avviene esclusivamente attraverso apparati dedicati e dotati di appositi filtri che impediscono l'accesso a siti a carattere pornografico, di violenza, razzista, ecc. Tuttavia il sistema di filtro non garantisce l'interdizione al 100% di determinati siti, pertanto l'utente si deve attenere comunque a quanto già indicato.

4. Il sistema registra i dati di traffico che, su richiesta dell'autorità giudiziaria, verranno messi a disposizione per le attività di indagine

5. E' facoltà dell'Amministrazione disporre di opportuni controlli del traffico web nel rispetto delle normative vigenti e del presente regolamento.

6. L'Ente può attivare apposite black list (siti interdetti alla navigazione dalla rete interna) al fine di impedire l'accesso a siti Internet non attinenti ai compiti di ufficio ed evitare gravi minacce e problemi per la sicurezza del sistema e delle informazioni in esso contenute.

CAPO IV

ART. 15 – ASSISTENZA – PROCEDURE OPERATIVE

1. Le procedure operative per le richieste di assistenza/servizio di cui al successivo comma sono regolate da apposita piattaforma di gestione delle richieste resa disponibile dal Servizio Sistemi Informativi attraverso la Intranet del Comune di Sanremo, previo assenso, ove necessario, del Dirigente o del Responsabile del Settore competente.

2. Il sistema di gestione delle richieste istruisce le principali richieste di assistenza/servizio, ovvero, a titolo esemplificativo e non esaustivo:
   - richiesta di assistenza per l'utilizzo delle procedure gestionali a disposizione dell'utente e distribuite dalla rete informatica;
   - richiesta di abilitazione accesso alla rete;
   - richiesta di creazione del profilo di posta elettronica e abilitazione all'accesso della casella di posta elettronica dell'ufficio;
   - richiesta di accesso alle informazioni presenti nelle cartelle condivise d'ufficio;
   - richiesta di creazione, modifica e cancellazione di un'utenza per l'accesso ai servizi della rete comunale;
   - richiesta di installazione di un nuovo applicativo;
   - richiesta di abilitazione ai servizi erogati sulla Intranet comunale per l'accesso a banche dati esterne;
   - richiesta di ripristino del personal computer, stampante o altro dispositivo fornito dall'ente;
   - richiesta di ripristino del funzionamento di software e programmi applicativi installati dall'ente.
   - Richiesta consumabili (toner, cartucce, nastri, etc.)

3. L'operatore del Servizio Sistemi Informativi prende in carico la Segnalazione per la valutazione tecnica a seguito della quale esegue l'intervento; qualora la richiesta lo necessiti l'operatore può chiedere ulteriori informazioni al Segnalatore; nel caso la richiesta sia palesemente errata o illecita l'operatore procederà a rifiutarla.

4. Qualora il sistema di "Helpdesk" non sia attivo, le richieste di cui al punto 2, dovranno pervenire al Servizio Sistemi Informativi tramite posta elettronica.

5. La presa in carico delle richieste di cui al punto 2 non è garantita qualora non venga rispettato l'iter descritto nel presente articolo.

6. Allo scopo di monitorare il corretto funzionamento dei personal computer, prevenendo quindi eventuali situazioni di guasto, può essere impiegato un controllo che permette di censire lo stato delle macchine in dotazione al personale. Il controllo non effettua in alcun modo registrazione di dati riguardanti l'attività degli utenti del PC, ma solo la registrazione di informazioni generiche sule caratteristiche hardware e i software installati (vedi ART. 14 comma 5).

CAPO V

ART. 16 – MODALITÀ DI CONTROLLO DA PARTE DEL COMUNE

1. L'Amministrazione si riserva di effettuare controlli sul corretto utilizzo degli strumenti informatici, della posta elettronica, di internet e delle apparecchiature telefoniche, nel rispetto delle normative vigenti e del presente regolamento.

2. Per esigenze organizzative, produttive e di sicurezza l'Amministrazione può avvalersi di strumenti che consentono un controllo a distanza di tipo generalizzato, indiretto e anonimo, relativo all'intera struttura amministrativa, ad aree, servizi o gruppi di utenti.

3. Qualora – durante un controllo generalizzato – vengano rilevate anomalie nell'utilizzo degli strumenti informatici, l'Amministrazione procede preliminarmente all'invio di un avviso generalizzato relativo all'uso improprio riscontrato, con l'invito ad attenersi scrupolosamente al presente regolamento e alla normativa vigente, e si riserva la facoltà di svolgere successive azioni mirate alla verifica del corretto utilizzo.

4. La violazione da parte degli utenti dei principi e delle norme contenute nel presente regolamento comporta l'applicazione delle sanzioni previste dalle disposizioni contrattuali vigenti in materia e, secondo quanto previsto dall'articolo 54 del Decreto Legislativo n. 165 del 30 Marzo 2001, dal Codice di Comportamento, previo espletamento del procedimento disciplinare.

5. L'Amministrazione si riserva di effettuare controlli difensivi, non rivolti cioè ad accertare l'attività lavorativa, ma eventuali condotte illecite del lavoratore, al fine dell'avvio del procedimento disciplinare in caso di uso non lecito degli strumenti.

6. Possibile accesso ai dati contenuti nella casella di posta elettronica individuale dell'utente

   6.1 Assenza programmata dell'utente

   Per prevenire la necessità di accedere alla casella di posta elettronica individuale dell'utente (dipendente e/o collaboratore) assente, il Comune di Sanremo ha messo a disposizione di costui apposite funzionalità di sistema, di agevole utilizzo, che consentono di inviare automaticamente, in caso di assenze (ad esempio, per ferie o attività di lavoro fuori sede) messaggi di risposta contenenti l'avviso dell'assenza, la data fino alla quale gli sarà impossibile leggere il messaggio e un riferimento alternativo aziendale (anche elettronico o telefonico) o altre utili modalità di contatto della struttura, per comunicazioni urgenti.
   Gli utenti devono avvalersi di tale funzionalità, prevenendo così l'apertura della posta elettronica.
   In merito fare riferimento alla procedura di cui al precedente fare riferimento all'art. 12 c.6.

   6.2 Assenza non programmata dell'utente

   In caso di eventuali assenze non programmate (ad esempio, per malattia), o comunque di sua impossibilità a consultare l'account (non solo di email) nella sua disponibilità, qualora il lavoratore non possa attivare la procedura sopra descritta, e perdurando l'assenza oltre un determinato limite temporale, il Comune di Sanremo potrebbe disporre lecitamente (al fine di garantire la sicurezza o comunque consentire la regolare continuità dell'attività aziendale), sempre che sia necessario e mediante personale appositamente incaricato, l'attivazione di analogo accorgimento, avvertendo gli interessati.

Sempre in assenza dell'utente interessato, nel caso in cui sussistano improrogabili necessità legate all'attività lavorativa, il Comune potrà verificare il contenuto sia della posta, sia di altri contenuti/comunicazioni ricevuti, secondo la procedura che segue.

Prima di attivare la procedura che segue, il Comune cercherà inoltre soluzioni alternative (non eccessivamente complicate), che possano consentire il recupero e la disponibilità del materiale occorrente al Comune stesso.

A titolo esemplificativo, cercherà di:
- verificare se nella lista di distribuzione del messaggio vi fossero altri dipendenti;
- richiedere nuovamente le informazioni da recuperare al mittente del messaggio.

Solo in caso di inapplicabilità di soluzioni alternative, si procederà con le seguenti modalità.
Su richiesta del Dirigente di riferimento, l'accesso alla casella di posta elettronica individuale del dipendente assente potrà avvenire direttamente, a cura dell'AdS, tramite autenticazione con nuove chiavi di accesso all'uopo generate.

In ogni caso, indipendentemente dalle soluzioni adottate, saranno validi i seguenti principi generali:

- ogni qualvolta sia necessario accedere alla casella di posta elettronica dell'utente assente (o impossibilitato, ecc.), al rientro gli verranno assegnate nuove chiavi di accesso temporanee;

- tutte le operazioni effettuate saranno registrate, a cura dell'Amministratore di Sistema, con specificazione della/e e-mail estratta/e, mediante la redazione di un verbale che verrà consegnato (anche via email o comunque tramite comunicazione elettronica) al lavoratore interessato al suo rientro.

6.3 Cessazione del rapporto professionale con l'utente

In caso di cessazione a qualsiasi titolo del rapporto professionale con il Comune di Sanremo, gli account di posta elettronica riconducibili a persone identificate o identificabili verranno rimossi, previa disattivazione degli stessi (entro tre mesi dal momento della cessazione del rapporto, onde impedire che l'immediata disattivazione possa recare pregiudizio all'Ente) e contestuale adozione di sistemi automatici volti ad informarne i terzi ed a fornire a questi ultimi indirizzi alternativi riferiti all'attività professionale del Comune.

Al termine dei 3 mesi, prima della cancellazione dell'account, verrà effettuata un'estrazione dei messaggi di posta dell'utente che verrà salvata su un volume crittografato e monitorato dai log di Sistema, accessibile esclusivamente dall'AdS, su esplicita richiesta del Titolare.

CAPO VI

ART. 17 – VIOLAZIONI

1. Qualsiasi utilizzo del sistema informativo dell'Ente non conforme alle disposizioni delle presenti norme operative e/o alle leggi vigenti è ad esclusiva responsabilità dell'Utente.
2. Ai fini della prevenzione degli accessi non autorizzati e degli abusi nell'utilizzo dei servizi offerti dal sistema informativo dell'Ente, saranno prese tutte le misure tecniche ed organizzative ritenute idonee, incluso l'utilizzo di strumenti automatici quali il monitoraggio degli accessi, gli strumenti di verifica del software e dell'hardware in uso sulle postazioni di lavoro e la registrazione dei collegamenti alle reti Intranet/Internet.
3. Nel pieno rispetto della normativa vigente, il Comune di Sanremo si riserva il diritto di verificare l'attuazione delle disposizioni delle presenti norme operative anche attraverso l'analisi del contenuto delle informazioni tracciate dagli strumenti di monitoraggio automatici.
4. Nei casi di accertata violazione delle presenti norme operative, è demandata ai rispettivi Dirigenti o all'ufficio di disciplina, l'applicazione dei necessari provvedimenti disciplinari, fermo restando l'obbligo di segnalare al Segretario Generale ed alla competente Autorità Giudiziaria eventuali violazioni costituenti reato.

ART. 18 - NOTE FINALI

1. Il presente disciplinare, è stato, prima della sua diffusione tra tutti gli utilizzatori di strumenti informatici e telematici messi a disposizione dall'Amministrazione comunale, oggetto di specifica preventiva informazione nei confronti dei lavoratori. Esso viene diffuso tra i dipendenti del Comune di Sanremo e adeguatamente pubblicizzato, oltre che nel sito web (internet e intranet) del Comune, a tutti gli utenti che facciano utilizzo di risorse strumentali informatiche dell'Ente.

2. I Responsabili dei Settori/Servizi/Unità Organizzative sono tenuti a vigilare affinché le presenti disposizioni siano comunicate a tutti gli utilizzatori delle risorse informatiche dell'Ente. Inoltre, il dipendente deve attenersi, nell'utilizzo e nella gestione delle risorse strumentali informatiche comunali, ai principi e ai doveri contenuti nel "Codice di comportamento dei dipendenti delle pubbliche amministrazioni" di cui al dpr n. 62/2013.

3. I documenti sopra richiamati (Deliberazione del Garante Privacy n.13/2007, dpr n. 62/2013 e Direttiva n.02/09 del Dipartimento della Funzione Pubblica) possono essere reperiti ai seguenti indirizzi internet:
   - http://www.garanteprivacy.it/garante/doc.jsp?ID=1387522
   - http://bancadati.digita-lex.it/public/files/pdf/0158_6-Direttiva_n2_09.pdf

4. Per ogni chiarimento Lei potrà rivolgersi al Segretario Comunale, al Responsabile dei Servizi Informativi – CED, agli amministratori di sistema:

Presa visione ed accettazione del Disciplinare

Il sottoscritto/a _____

Nato/a _____

Residente a _____ in _____

Telefono _____ Codice fiscale _____

Data _____ Firma _____

APPENDICE 1 – SCELTA DELLA PASSWORD

Il primo passo per proteggere la privacy online è la creazione di una password sicura, ovvero una password che non possa essere scoperta da un programma o una persona in un breve lasso di tempo.

Alcuni suggerimenti per creare una password sicura, presi dal sito della Polizia Postale:

- Creare una password di minimo dieci caratteri, contenente almeno una maiuscola, almeno una minuscola, almeno un numero e almeno un carattere speciale tra quelli elencati di seguito:
  ! $? # = * + - . , ; :
- Includere caratteri dall'apparenza simili in sostituzione di altri caratteri (ad esempio il numero "0" per la lettera "O" o il carattere "$" per la lettera "S").
- Creare un acronimo univoco (ad esempio "PDRM" per "Piazza Delle Repubbliche Marinare").
- Includere sostituzioni fonetiche o grafiche (ad esempio "6 arrivato" per "Sei arrivato" o "Arrivo + tardi" per "Arrivo più tardi").

Da evitare:

- Non utilizzare le stesse password per più account.
- Non usare una password già utilizzata in un esempio di come si sceglie una buona password.
- Non utilizzare una password contenente dati personali (nome, data di nascita, ecc.)
- Non usare parole o acronimi che si possono trovare nel dizionario.
- Non usare sequenze di tasti sulla tastiera (asdf) o sequenze di numeri (1234).
- Non creare password di soli numeri, di sole lettere maiuscole o di sole lettere minuscole.
- Non usare ripetizioni di caratteri (aa11).

Suggerimenti per tenere al sicuro la password:

- Non comunicare a nessuno la password (inclusi partner, compagni di appartamento, colleghi, ecc.).
- Non lasciare la password scritta in posti facilmente raggiungibili da altri.
- Non inviare mai la password per e-mail.

Verificare periodicamente la password corrente e cambiarla con una nuova.

ALLEGATO - GLOSSARIO DEI TERMINI TECNICI

Termine	Significato
Account	Iscrizione registrata su un server e che, tramite l'inserimento di una userId e di una password, consente l'accesso alla rete e/o ai servizi. Ad esempio, un account ci permette di entrare in Internet, un altro account ci serve per ricevere e spedire posta elettronica. Un account ci consente di accedere alle risorse di una rete locale, come server, file server, stampanti. Altri account servono per accedere a server e servizi vari.
Antivirus	Tipo di software che cerca e distrugge gli eventuali programmi virus e cerca di rimediare ai danni che gli stessi virus hanno compiuto.
Backup	Copia di riserva di disco, di una parte del disco o di uno o più file.
Black list	Elenco di siti considerati non opportuni per l'espletamento delle funzioni lavorative dell'Amministrazione.
Database (Base Dati).	Qualsiasi aggregato di dati organizzato in campo (colonne) e record (righe).
Download	Registrare sul proprio disco rigido un file richiamandolo, tramite modem o rete, da un computer, da un server o da un host (tramite Internet, rete locale o geografica).
E-mail Electronic mail, posta elettronica.	Scambio di messaggi e di file attraverso una rete locale o Internet. Avviene in tempo reale ed è indipendente dalla posizione fisica dei computer mittente e destinatario. I messaggi e file vengono conservati da un server che provvede ad inoltrarli al destinatario quando questo si collega.
Firewall	Insieme di software/hardware usato per filtrare i dati in scambio fra reti diverse, al fine di proteggere un server da attacchi pervenuti via rete locale o via Internet. Consente il passaggio solamente di determinati tipi di dati, da determinati terminali e determinati utenti.
Freeware	Software gratuito realizzato e distribuito da privati o piccole società, attraverso Internet o CD- ROM allegati a pubblicazioni in edicola.
Hardware	Letteralmente ferramenta, in informatica si intende l'insieme dei componenti (CPU, Hard Disk ecc.) che costituiscono un computer.
HelpDesk	Risorsa informativa e di assistenza che prende in carico i problemi che sorgono nell'uso del sistema informativo comunale.
Internet	La madre di tutte le reti di computer. E' l'insieme mondiale delle reti di computer interconnesse.
Intranet	La Intranet è una rete locale (Local Area Network), o un raggruppamento di reti locali, usata all'interno di una organizzazione per facilitare la comunicazione e l'accesso alle informazioni
MP3 (MPEG-4)	Tecnologia per la compressione/decompressione di file audio/video che consente di mantenere una perfetta fedeltà e qualità anche riducendo i file di ben 11 volte la grandezza originale.
MPG (Motion Picture Experts Group)	Stabilisce gli standard digitali per audio e video. E' in particolare lo standard di compressione utilizzato per codificare i video registrati su DVD.
Password	Parola che consente l'accesso di un utente ad una rete, ad un servizio telematico o ad un sito Internet. E' necessario digitarla esattamente (caratteri maiuscoli/minuscoli), assieme alla user-id.

Quicktime	Standard definito dalla Apple e utilizzato da tutti i computer per la riproduzione fedele dei filmati video.
CED Centro Elaborazione Dati	Servizio che, nell'ambito dell'Amministrazione, si occupa di impostare, indirizzare e coordinare l'introduzione delle tecnologie informatiche nell'attività del Comune, ponendosi quale punto di riferimento tecnologico per la definizione delle strategie di evoluzione e innovazione dei Sistemi Informativi.
Software	Sono i programmi (professionali, ludici, video, musicali, raccolte di suoi ed immagini) per i computer.
Streaming	Con il termine streaming si intende un flusso di dati audio/video trasmessi da una sorgente a una o più destinazioni su Internet.
Url filtering	Sistema che permette di monitorare e filtrare la navigazione in Internet, bloccando l'accesso a particolari categorie di siti, al fine di limitare il rischio di utilizzo improprio della rete e la navigazione in siti non pertinenti o non compatibili con l'attività aziendale.
User Id, Nome utente, Utente (User)	Chiunque utilizzi un elaboratore collegato alla rete, sia che il collegamento avvenga in rete locale sia che si tratti di un accesso remoto.
Virus	Un programma creato per diffondersi da computer a computer, spesso danneggiando i dati e gli altri programmi registrati.
White list	Elenco di siti considerati opportuni per l'espletamento delle funzioni lavorative dell'Amministrazione.