COMUNE DI CAMPOLONGO MAGGIORE

Provincia di Venezia

DISCIPLINARE
PER L'UTILIZZO DI INTERNET E DELLA POSTA ELETTRONICA

Indice

Approvato con deliberazione della Giunta Comunale n. 79 del 22.9.2009

1. OGGETTO

1. Il presente disciplinare, adottato sulla base delle indicazioni contenute nel provvedimento di data 1 marzo 2007 (in G.U. n. 58 di data 10 marzo 2007) del Garante per la protezione dei dati personali, riguardante il *Trattamento di dati personali relativo all'utilizzo di strumenti elettronici da parte dei lavoratori*, e nella Direttiva n. 2/09 del Ministro per la Pubblica Amministrazione e l'Innovazione del 26.5.2009 recante *Utilizzo di Internet e della casella di posta elettronica istituzionale sul luogo di lavoro*, ha per oggetto i criteri e le modalità operative di accesso e di utilizzo del servizio internet e di posta elettronica da parte dei dipendenti e degli Amministratori del Comune di Campolongo Maggiore, e di tutti gli altri soggetti che a vario titolo operano nelle strutture dell'ente (lavoratori socialmente utili, collaboratori, tirocinanti, stagisti etc.).

2. DEFINIZIONI

1. Nel presente documento si intende per:
   - SERVIZIO INTERNET: accesso telematico alla rete mondiale di computer;
   - UTENTE INTERNET (BASE): persona autorizzata ad accedere alla lista (white list) di siti istituzionali preventivamente selezionati dall'Amministrazione comunale;
   - UTENTE INTERNET (AMPIO): persona autorizzata ad accedere al servizio internet al di là dei siti istituzionali preventivamente selezionati dall'Amministrazione comunale, con l'unico limite di filtri predeterminati che si attivano in modo automatico durante la navigazione;
   - WHITE LIST: elenco di siti direttamente e immediatamente accessibili da tutti gli utenti internet (base);
   - BLACK LIST: elenco di siti non accessibili agli utenti;
   - SERVIZIO DI POSTA ELETTRONICA: l'invio e la ricezione (a/da utenti) di messaggi contenenti testo ed altri formati (es.: immagini, video, audio).
   - SERVIZIO DI POSTA ELETTRONICA CERTIFICATA (PEC): l'invio e la ricezione (a/da utenti) di messaggi contenenti testo ed altri formati (es.: immagini, video, audio) con la garanzia del ricevimento del messaggio da parte del destinatario e della integrità del messaggio ricevuto. Il servizio è equiparato a tutti gli effetti di legge alla spedizione di una raccomandata cartacea con avviso di ricevimento.
   - UTENTE DI POSTA ELETTRONICA: persona autorizzata ad accedere al servizio di posta elettronica;
   - UTENTE DI POSTA ELETTRONICA CERTIFICATA (PEC): persona autorizzata ad accedere al servizio di posta elettronica certificata;
   - INTERNET PROVIDER: azienda che fornisce all'ente l'accesso alla rete internet;
   - POSTAZIONE DI LAVORO: personal computer collegato alla rete comunale tramite il quale l'utente accede ai servizi informatici e telematici;
   - LOG: archivio delle attività di consultazione in rete;
   - RESPONSABILE DELLA SICUREZZA: progetta, realizza e mantiene in efficienza le misure di sicurezza, conformemente a quanto previsto dagli articoli 31 e 33 del Dlgs 196/2003.
   - AMMINISTRATORE DI SISTEMA: garantisce agli utenti supporto tecnico per l'accesso ed il corretto utilizzo dei servizi internet e di posta elettronica, conformemente a quanto previsto dall'art. 154, comma 1, lett. c) ed h) del Dlgs 196/2003.

3. GESTIONE DEI SERVIZI TELEMATICI

1. I servizi Internet e di posta elettronica sono assicurati e gestiti dall'Ufficio Informatica, cui è assegnata la responsabilità del loro corretto funzionamento.
2. In particolare, l'Ufficio Informatica è tenuto a:

- adottare le misure più idonee a garantire la continuità, la disponibilità e la sicurezza dei servizi;
- gestire i dati degli utenti nel rispetto della vigente normativa sulla tutela dei dati personali;
- informare tempestivamente gli utenti, con un anticipo almeno di 24 ore, su eventuali interruzioni dei servizi telematici che si rendessero necessarie per cause di forza maggiore;
- monitorare i livelli dei servizi telematici al fine di garantirne la massima efficienza;
- monitorare l'utilizzo dei servizi telematici da parte degli utenti al fine di evidenziarne usi scorretti o non consentiti;
- offrire assistenza tecnica agli utenti.

3. L'Ufficio Informatica provvede altresì a:

- ad attivare presso ogni postazione di lavoro l'accesso ad Internet;

- ad attivare, per ogni nuovo dipendente assunto in servizio in servizio, una casella di posta elettronica personale. Parimenti l'Ufficio Informatica provvede a disattivare la casella di posta elettronica personale del dipendente cessato dal servizio;
- ad attivare/disattivare caselle di posta elettronica per il Sindaco e gli Assessori;
- ad attivare/disattivare caselle di posta elettronica per i collaboratori, previa richiesta del Responsabile dell'Area di riferimento;
- ad attivare/disattivare le caselle di posta elettronica di struttura a seguito di ogni modifica organizzativa dell'ente;
- ad attivare/disattivare le caselle di PEC.

4. L'attivazione di una casella di posta elettronica è effettuata attraverso l'assegnazione di un codice identificativo dell'utente (userid), la relativa parola chiave riservata (password) iniziale, ed un indirizzo.
5. Gli indirizzi di posta elettronica per le caselle personali hanno la seguente nomenclatura, salvo casi di omonimia od esigenze particolari: nomeutente.cognomeutente@comune.campolongo.ve.it
6. Gli indirizzi di posta elettronica per le caselle personali degli Amministratori hanno la seguente nomenclatura, salvo casi di omonimia od esigenze particolari: nomefunzione@comune.campolongo.ve.it
7. Gli indirizzi di posta elettronica per le caselle di struttura hanno la seguente nomenclatura, salvo casi particolari: nomestruttura@comune.campolongo.ve.it
8. Gli indirizzi di PEC, sia per quanto riguarda le caselle personali che quelle di struttura, si adeguano alle disposizioni precedenti salvo che per il dominio, la cui nomenclatura viene definita dal fornitore del servizio.
9. L'Ufficio Informatica non effettua alcun controllo, censura, modifica, cancellazione dei messaggi di posta elettronica ricevuti e inviati dagli utenti, a meno che ciò non venga richiesto dalla legge ovvero non sia disposto dall'autorità giudiziaria.

4. MODALITA DI UTILIZZO DEL SERVIZIO INTERNET

1. Per ridurre il rischio di usi impropri nell'utilizzo di internet, l'ente adotta opportune misure tese a prevenire controlli successivi sul lavoratore.
2. Per accedere ai servizi informatici e telematici comunali da una qualsiasi postazione di lavoro l'utente dovrà utilizzare un codice identificativo (id. utente) e una parola chiave segreta (password). Superato il sistema di autenticazione l'utente sarà collegato alla rete comunale e ad internet senza ulteriori formalità.
3. Tutti i dipendenti, gli amministratori e gli altri soggetti che a vario titolo operano nelle strutture dell'ente possono utilizzare internet, limitatamente ad una lista di siti istituzionali preventivamente individuati dal Responsabile alla sicurezza di concerto con l'Amministratore di sistema (WHITE LIST) e previa identificazione con le modalità sopra illustrate (id. utente/password).
4. La lista dei siti (WHITE LIST) sarà implementata nel tempo a cura dell'Ufficio informatica anche su richiesta dei diversi Responsabili d'Area.
5. L'utilizzo ampio di internet, non limitato cioè alla lista dei siti istituzionali, è libero per i Responsabili d'Area, il Segretario Generale e gli Amministratori, mentre sarà autorizzato per ogni singolo utente dal Responsabile, previa richiesta motivata dei dirigenti.
6. Al fine di prevenire il rischio di utilizzi impropri della rete, l'ente utilizza un sistema di filtri che impediscono l'accesso diretto a siti che sicuramente non hanno natura istituzionale (BLACK LIST) .
7. Oltre a tale sistema, è attiva una funzione di verifica del contenuto del sito; ove tale contenuto, secondo l'impostazione di una soglia predefinita di filtri, appaia non istituzionale viene visualizzato un messaggio che avverte l'utente; per rendere disponibile la pagina sarà necessaria l'autorizzazione del Responsabile della Sicurezza, e l'inserimento del sito nella WHITE LIST da parte del Servizio informatica.
8. Le modalità di individuazione e di applicazione dei filtri sono concordate dal Responsabile della Sicurezza con l'Amministratore di sistema.
9. L'utente è direttamente e totalmente responsabile dell'uso che egli fa del servizio di accesso a internet, dei contenuti che vi ricerca, dei siti che contatta, delle informazioni che vi immette e delle modalità con cui opera.
10. Lo scarico di immagini, di file audio o musicali, di file video e in ogni casi di grandi quantità di dati in grado di degradare le prestazioni offerte dal servizio agli altri utenti può avvenire solo in casi eccezionali, su espressa autorizzazione del Responsabile della sicurezza e Amministratore di Sistema, e in fasce orarie di basso utilizzo del canale internet (dalle ore 12.00 alle ore 14.30. e dopo le 17.00).
11. All'utente non è consentito:

- servirsi o dar modo ad altri di servirsi della stazione di accesso a internet per attività non istituzionali, per attività poste in essere in violazione del diritto d'autore o altri diritti tutelati dalla normativa vigente;

- utilizzare sistemi Peer to Peer (P2P), chat, file sharing, podcasting, webcasting o similari, così come connettersi a siti che trasmettono programmi in streaming (come radio o TV via WEB) senza essere stati preventivamente autorizzati dall'Ufficio informatica;
- scaricare software dalla rete; eventuali necessità dovranno essere appositamente richieste all'Ufficio Informatica che, dopo aver verificato il rispetto delle condizioni di licenza, provvederà a eseguire fisicamente lo scarico in modalità sicura e consegnare il software al richiedente;
- utilizzare internet provider diversi da quello scelto ufficialmente dall'ente e la connessione di stazioni di lavoro aziendali alle reti di detti provider con sistemi diversi (es. modem) da quello centralizzato;
- usare la rete in modo difforme da quanto previsto dal presente disciplinare e dalle leggi penali, civili ed amministrative in materia.

5. MODALITA' DI UTILIZZO DEL SERVIZIO DI POSTA ELETTRONICA

1. Il servizio di posta elettronica è operante con continuità 24 ore al giorno per 365 giorni l'anno.
2. L'utilizzo del servizio di posta elettronica è consentito solo per ragioni di servizio agli utenti identificati con le modalità di cui all'articolo precedente.
3. L'ente fornisce:

- a tutti i propri dipendenti, al Sindaco e agli Assessori una casella di posta elettronica personale (casella personale);
- ai Responsabili d'Area, al Segretario e al Sindaco una casella di posta elettronica certificata PEC;

4. L'ente fornisce altresì alle proprie strutture le caselle di posta elettronica e di PEC (caselle istituzionali) ritenute utili.
5. L'ente può fornire una casella di posta elettronica ai propri collaboratori, previa richiesta del Responsabile della struttura di afferenza.
6. Gli utenti hanno l'obbligo di procedere alla tempestiva lettura della corrispondenza pervenuta nella propria casella, almeno una volta al giorno.
7. Le caselle istituzionali sono accessibili solo in modalità di delega, previa richiesta e autorizzazione del Responsabile della sicurezza.
8. In caso di assenza dal lavoro dell'utente per brevi periodi, è a disposizione una apposita funzionalità di sistema che consente di inviare automaticamente un messaggio di risposta che avvisa il mittente dell'assenza del destinatario, individuando eventualmente altre modalità di contatto con la struttura.
9. In caso di assenza non programmata o dove non sia stata attivata la procedura di cui sopra, l'utente può delegare un altro dipendente dell'ufficio a verificare il contenuto dei messaggi e ad inoltrare al Responsabile dell'Area quelli ritenuti rilevanti e per lo svolgimento dell'attività lavorativa.
10. L'utente, nell'utilizzo del servizio di posta elettronica è tenuto a conformarsi alle indicazioni tecniche fornite all'Ufficio Informatica ed ad attenersi alle prescrizioni che seguono:
    a. non utilizzare la posta elettronica per trasmettere e diffondere materiali la cui distribuzione sia illegale;
    b. non usare il servizio per scopi illegali, per inviare o ricevere materiale pornografico, osceno, volgare, diffamatorio, oltraggioso, discriminatorio, abusivo, pericoloso;
    c. non inviare e ricevere materiali e/o messaggi che incoraggino terzi a mettere in atto una condotta illecita e/o criminosa passibile di responsabilità penale o civile;
    d. non utilizzare il servizio per inviare catene di lettere, solleciti commerciali, messaggi politici ovvero qualunque altro messaggio a persone che non abbiano acconsentito a tale procedura;
    e. non utilizzare il servizio per motivi privati e/o per contatti interpersonali tra i dipendenti non inerenti l'uso d'ufficio;
    f. non inviare giochi, scherzi, barzellette, appelli e petizioni
    g. non allegare al testo delle comunicazioni materiale potenzialmente insicuro (ad es. programmi, scripts, macro), così come file di dimensioni eccedenti i limiti indicati dall'Ufficio Informatica
    h. non inviare messaggi ad una pluralità di destinatari (mail spamming) indiscriminatamente, eccedenti il numero dei reali interessati;
    i. utilizzare con diligenza il servizio, evitando di sovraccaricare il sistema con l'invio di messaggi ed allegati di dimensioni inutilmente eccessive e/o contenenti inutili grafismi od immagini;
    j. cancellare messaggi ricevuti inutili e di dimensioni eccessive;
    k. utilizzare il servizio nel pieno rispetto del Codice di tutela dei dati personali;
    l. adottare le necessarie cautele per assicurare la segretezza del proprio userid e della propria password; ovemai, sotto la sua personale responsabilità, le registri su un supporto qualsiasi, deve custodirle con la massima diligenza;

m. scegliere password non banali o comunque non contenenti riferimenti agevolmente riconducibili alla sua identità.

11. L'utilizzo di liste di distribuzione riservate, comunemente riunite nella "Rubrica gruppi", che permettono l'invio di e–mails a una pluralità di utenti o a tutti gli utenti, è consentito solo a determinati soggetti, su autorizzazione del Responsabile della Sicurezza.
12. Agli utenti è consentito utilizzare, per ragioni personali, servizi di posta elettronica o di rete (webmail) fuori dall'orario di lavoro o durante le pause, ovvero, moderatamente, anche nel tempo di lavoro.

6. RESPONSABILITA' DEGLI UTENTI NELL'UTILIZZO DEI SERVIZI TELEMATICI

1. La configurazione dei servizi di accesso ad internet e di posta elettronica viene eseguita esclusivamente dai tecnici dell'Ufficio Informatica.
2. Per accedere ai servizi informatici comunali da una postazione di lavoro l'utente dovrà utilizzare un codice identificativo (id. utente) e una parola chiave segreta (password). Superato il sistema di autenticazione l'utente sarà collegato alla rete comunale e ad internet senza ulteriori formalità.
3. Le postazioni di lavoro sono preventivamente individuate ed assegnate personalmente a ciascun utente. L'accesso alla rete da una postazione diversa da quella assegnata avviene solo in caso di particolari e temporanee esigenze di servizio previo inserimento del proprio codice identificativo - id. utente - e della propria password personale.
4. Per ragioni di riservatezza l'utente si impegna a:
   a. non cedere, una volta superata la fase di autenticazione, l'uso della propria stazione a personale non autorizzato, in particolar modo per quanto riguarda l'accesso a internet e ai servizi di posta elettronica;
   b. non lasciare incustodita ed accessibile la propria postazione una volta connessi al sistema con le proprie credenziali;
   c. conservare la password nella massima riservatezza e con la massima diligenza;
   d. non utilizzare credenziali (user-id e password) di altri utenti, nemmeno se fornite volontariamente o di cui si è venuti casualmente a conoscenza;
   e. mantenere la corretta configurazione del proprio computer non alterando le componenti hardware e software predisposte allo scopo, né installando ulteriore software non autorizzato;
   f. non salvare file audio, video e file non istituzionale qualsiasi tipo nelle connessioni di rete (ad esempio K: - S:) su cui viene eseguito giornalmente il back-up.
5. Per prevenire la manomissione della configurazione hardware e software delle postazioni di lavoro, salvo rari casi necessari per il funzionamento di specifici applicativi, gli utenti sono configurati con diritti limitati (diversi da quelli di amministratore). Per l'installazione di software o la modifica della configurazioni è necessario l'intervento dell'Amministratore di Sistema
6. E' in ogni caso vietata qualsiasi attività illecita, o che comunque possa produrre danni alle risorse informatiche dell'ente. A titolo esemplificativo, costituisce violazione:
   - qualsiasi azione che possa compromettere la sicurezza e la riservatezza delle risorse informatiche dell'ente, o di altri organismi, accessibili attraverso le medesime risorse.
   - l'accesso, l'utilizzazione, la distruzione, l'alterazione o la disabilitazione non autorizzata di risorse informatiche anche mediante credenziali di accesso rese disponibili da altre soggetti, nonché l'abbandono senza custodia o senza protezione di stazioni di lavoro già connesse alla rete;
   - l'uso di dati o di altre risorse informatiche per scopi non consentiti dal presente Disciplinare;
   - l'utilizzo per scopi di interesse esclusivamente privato di qualsiasi risorsa dell'ente;
   - qualunque altra attività in contrasto con il presente Disciplinare.
7. Qualsiasi operazione svolta utilizzando un determinato codice identificativo e/o password sarà ricondotta alla responsabilità dell'utente assegnatario del medesimo codice. L'utente stesso sarà dunque ritenuto civilmente e penalmente responsabile di qualsiasi danno arrecato all'ente e all'internet provider, nonché delle eventuali conseguenze pregiudizievoli che un uso improprio del servizio da parte del proprio userid potrebbero comportare a terzi .
8. La violazione delle disposizioni di cui al presente atto comporta l'applicazione delle sanzioni disciplinari previste dal vigente CCNL, salva ogni ulteriore forma di responsabilità civile e penale.

7. MONITORAGGIO E CONTROLLI

1. L’ente può riservarsi di controllare, per il tramite dell’Amministratore di sistema, l'effettivo adempimento della prestazione lavorativa e, se necessario, il corretto utilizzo degli strumenti di lavoro. Nell'esercizio di tale prerogativa, e nel rispetto della libertà e la dignità dei lavoratori, è vietata l’installazione di apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori, tra cui sono certamente comprese strumentazioni hardware e software mirate al controllo dell'utente di un sistema di comunicazione elettronica.
2. L’ente, utilizzando sistemi informativi per esigenze produttive o organizzative (ad es., per rilevare anomalie o per manutenzioni) o, comunque, quando gli stessi si rivelano necessari per la sicurezza sul lavoro, può avvalersi legittimamente, nel rispetto dello Statuto dei lavoratori, di sistemi che consentono indirettamente un controllo a distanza (c.d. controllo preterintenzionale) e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori. Ciò, anche in presenza di attività di controllo discontinue.
3. L’ente rispetta le procedure di informazione e di consultazione di lavoratori e sindacati in relazione all'introduzione o alla modifica di sistemi automatizzati per la raccolta e l'utilizzazione dei dati, nonché in caso di introduzione o di modificazione di procedimenti tecnici destinati a controllare i movimenti o la produttività dei lavoratori.
4. Nell'effettuare controlli sull'uso degli strumenti elettronici deve essere evitata un'interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata.
5. L'eventuale controllo è lecito solo se sono rispettati i principi di pertinenza e non eccedenza.
6. Nel caso in cui un evento dannoso o una situazione di pericolo non siano stati impediti con preventivi accorgimenti tecnici, l’ente adotta le misure di seguito indicate per consentire la verifica di comportamenti anomali.
7. I dati di accesso ad internet vengano automaticamente registrati in forma elettronica attraverso i LOG di sistema.
8. Il trattamento dei dati contenuti nei LOG potrà avvenire esclusivamente in forma anonima in modo tale da precludere l’identificazione degli utenti e/o delle loro attività. I dati anonimi aggregati, riferibili all’intera struttura o a sue aree, sono a disposizione dell’Amministratore di sistema per le valutazioni di competenza e riguarderanno:
   - Per ciascun sito/dominio visitato: il numero di utenti che lo visitano, il numero delle relative pagine richieste e della quantità di dati da lì scaricati;
   - Per ciascun utente: il numero di siti visitati, la quantità totale di dati scaricati, e le postazioni di lavoro utilizzate per la navigazione.
9. Il controllo anonimo può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. L'avviso può essere circoscritto a dipendenti afferenti all'Area in cui è stata rilevata l'anomalia. In assenza di successive anomalie non è di regola giustificato effettuare controlli su base individuale.
10. I dati personali contenuti nei log potranno essere trattati in via eccezionale e tassativamente nelle seguenti ipotesi:
    - Per corrispondere ad eventuali richieste della polizia postale e/o dell’autorità giudiziaria;
    - Su richiesta del Responsabile della sicurezza quando si verifichi un evento dannoso o una situazione di pericolo che richieda un immediato intervento;
    - Su richiesta dell’Amministratore di sistema limitatamente al caso di utilizzo anomalo degli strumenti da parte degli utenti di una specifica struttura/area (rilevabile esclusivamente dai dati aggregati) e reiterato il mese successivo nonostante un necessario esplicito invito agli utenti da parte del Responsabile della sicurezza ad attenersi ai compiti assegnati ed alle istruzioni impartite.
11. E’ in ogni caso esclusa l'ammissibilità di controlli prolungati, costanti o indiscriminati
12. I dati contenuti nei LOG sono conservati per il tempo strettamente necessario al perseguimento di finalità organizzative, produttive e di sicurezza, comunque non superiore a 12 mesi, e sono periodicamente cancellati automaticamente dal sistema.
13. I contenuti dei messaggi di posta elettronica, come pure i dati esteriori delle comunicazioni e i files allegati, sono riservati, e in nessun caso possono essere oggetto di verifica, controllo o censura da parte dell’ente, dell’internet provider o di altri soggetti.
14. I dati riguardanti il software installato sulle postazioni di lavoro (senza alcuna indicazione dell’utente che ha effettuato l’installazione) possono essere trattati per finalità di verifica della sicurezza dei sistemi ed il controllo del rispetto delle licenze regolarmente acquistate.

8. INTERRUZIONE E SOSPENSIONE DEI SERVIZI TELEMATICI

1. Previo adeguato preavviso, allo scopo di consentire lo svolgimento di interventi di manutenzione ordinaria e straordinaria del sistema l'Ufficio Informatica può disporre la sospensione temporanea dei servizi telematici.
2. Salvo più gravi responsabilità di ordine disciplinare, civile e penale, l'utilizzo dei servizi telematici sarà sospeso d'ufficio nei seguenti casi:
   - cessazione dall'impiego dell'utente;
   - accertata violazione, purché reiterata, delle disposizioni di cui al precedente art. 6, commi 4 e 6;
   - accertato accesso doloso dell'utente a directory, a siti e/o file e/o servizi da chiunque resi disponibili non rientranti fra quelli per lui autorizzati, e in ogni caso qualora l'attività dell'utente comporti danno, anche solo potenziale, al sito contattato;
   - in caso di concessione di accesso ad internet diretta o indiretta a qualsiasi titolo da parte dell'utente a terzi;
   - in caso di violazione e/o inadempimento imputabile all'utente di quanto stabilito nei precedenti punti;
   - in ogni altro caso in cui sussistano ragionevoli evidenze di una violazione degli obblighi dell'utente.

9. DOVERE DI INFORMAZIONE

1. Compete all'ente assicurare la corretta e preventiva informazione agli interessati su eventuali trattamenti di dati che possono riguardarli.
2. Quando sorga la necessità di un trattamento lecito dei dati, il Responsabile della sicurezza ne dà formale comunicazione all'interessato indicando le finalità connesse a specifiche esigenze organizzative, produttive e di sicurezza del lavoro, nonché le principali caratteristiche dei trattamenti, che possono anche riguardare l'esercizio di un diritto in sede giudiziaria.
3. Per l'esercizio dei propri diritti i lavoratori possono rivolgersi al Responsabile della sicurezza.

10. DISPOSIZIONI FINALI

1. Per quanto non previsto nel presente Disciplinare si applicano le disposizioni contenute nel provvedimento di data 1 marzo 2007 (in G.U. n. 58 di data 10 marzo 2007) del Garante per la protezione dei dati personali, riguardante il *Trattamento di dati personali relativo all'utilizzo di strumenti elettronici da parte dei lavoratori*, e nella Direttiva n. 2/09 del Ministro per la Pubblica Amministrazione e l'Innovazione del 26.5.2009 recante *Utilizzo di Internet e della casella di posta elettronica istituzionale sul luogo di lavoro*.
2. Il presente Disciplinare è soggetto a periodici aggiornamenti che dovessero rendersi opportuni a seguito di innovazioni organizzative, normative o tecnologiche.

11. ENTRATA IN VIGORE

1. Il presente Disciplinare entra in vigore ad avvenuta esecutività della deliberazione che lo approva.

12. DIFFUSIONE

1. Copia del presente Disciplinare è trasmessa per via telematica a tutti gli utenti dei servizi telematici.
2. Copia del presente Disciplinare è pubblicata all'Albo dei dipendenti ai sensi dell'art. 3, comma 10 del CCNL 2006-2009.
3. Copia del presente Disciplinare è pubblicata sul sito telematico comunale, per la dovuta pubblicità.