Comune di Nola
Provincia di Napoli

Disciplinare interno per l'utilizzo di Internet e posta elettronica da parte dei dipendenti

Sommario

Adottato con Delibera di G.M. n. 201 del 12/05/2011

1. Oggetto

Con riferimento al Provvedimento del Garante per la Protezione dei Dati Personali 1 marzo 2007 (in G.U. n. 58 del 10 marzo 2007), è adottato il presente disciplinare, avente ad oggetto la precisa definizione di criteri e modalità di accesso ed utilizzo ai servizi Internet e posta elettronica da parte del personale dipendente del Comune di Nola e di tutti i soggetti che a vario titolo operano nelle strutture del Comune.

2. Modalità di utilizzo delle postazioni di lavoro

L'accesso alla rete aziendale e ad internet sono concessi agli utenti autenticati e nei limiti stabiliti per ciascun profilo di utenza.

Per accedere ai servizi informatici da una postazione di lavoro l'utente deve necessariamente ed obbligatoriamente autenticarsi, utilizzando un codice identificativo (codice utente) e una parola chiave segreta (password).

L'utente, tenuto conto che la conoscenza della password da parte di terzi può consentire agli stessi l'accesso alla rete aziendale in nome dell'utente titolare e l'accesso ai dati cui il medesimo è abilitato (ad es. visualizzazione di informazioni riservate, distruzione o modifica dei dati, lettura della posta elettronica, uso indebito di servizi, ecc.), ha l'**obbligo** di:

- non cedere, una volta superata la fase di autenticazione, l'uso della propria postazione a persone non autorizzate, in particolar modo per quanto riguarda l'accesso a Internet e ai servizi di posta elettronica,
- non lasciare incustodita ed accessibile la propria postazione una volta connesso al sistema con le proprie credenziali di autenticazione, provvedendo a bloccare la postazione in caso di allontanamento temporaneo,
- conservare la password nella massima *riservatezza* e con la massima diligenza,
- avvisare prontamente il ***Servizio Informativo Comunale (SIC)*** nell'ipotesi di smarrimento dei dati di accesso,
- non utilizzare credenziali (codice utente e password) di altri utenti, nemmeno se fornite volontariamente o di cui si ha casualmente conoscenza,
- cambiare la propria password secondo le istruzioni ricevute.

L'utente ha l'obbligo di mantenere la corretta configurazione della propria postazione di lavoro, ***non alterando le componenti hardware e software e non installando ulteriore software non autorizzato***. Ogni eventuale modifica, connessa a problematiche ed esigenze di operatività lavorativa, dovrà essere richiesta al *SIC*.

3. Misure tecnologiche e organizzative

In ottemperanza al provvedimento del Garante del 01/03/2007, l'ente ha provveduto ad adottare le misure organizzative previste al punto 5.2. e segnatamente:

- ha proceduto ad un'attenta valutazione dell'impatto sui diritti dei lavoratori, in particolare adottando misure tecnologiche preventive e automatiche che limitano fortemente la necessità di ricorrere a controlli puntuali e individuali;
- ha individuato i lavoratori cui è accordato l'utilizzo della posta elettronica e l'accesso a Internet;
- ha individuato quale ubicazione è riservata alle postazioni di lavoro, agli apparati di rete e ai server, al fine di ridurre il rischio di impieghi abusivi.

4. Navigazione Internet

L'utilizzo di Internet è permesso esclusivamente in relazione a finalità istituzionali e connesse all'attività lavorativa.

Al fine di limitare allo stretto necessario i controlli sull'utilizzo corretto della navigazione su Internet, il Comune ha predisposto l'installazione di dispositivi perimetrali che *filtrano l'accesso alla rete ed inibiscono il collegamento a siti considerati non appropriati*.

Tale modalità di *web filtering* è basata sull'utilizzo di categorie e liste di siti bloccati (*black list*), periodicamente aggiornate. L'utente che tentasse di collegarsi a siti inclusi in tali *black list* riceve un avviso che lo informa di aver tentato un accesso ad una risorsa considerata non appropriata.

Le categorie bloccate (*black list*) sono, ad esempio, quelle che rappresentano siti pedo-pornografici, siti di scommesse e giochi on-line ed altri siti considerati non funzionali all'attività lavorativa, illegali o rischiosi.

In caso di blocco di un sito considerato erroneamente incluso nella *black list*, l'utente può comunicare tale circostanza al *SIC,* che provvederà, eseguiti gli opportuni controlli, a richiedere un eventuale sblocco.

Per gli utenti che accedono a Internet è vietato:

- eludere in qualsiasi modo i sistemi di controllo e filtraggio automatico;
- reiterare tentativi di accesso a siti bloccati e di cui si è avuta evidenza del fatto che si tratta di siti non appropriati e non consentiti;
- servirsi delle postazioni di accesso a Internet per attività non istituzionali e non connesse ad attività lavorative e per attività poste in essere in violazione del diritto d'autore o altri diritti tutelati dalla normativa vigente;
- danneggiare, distruggere, cercare di accedere senza autorizzazione ai dati o violare la riservatezza di altri utenti, compresa l'intercettazione o la diffusione di parole di accesso (password), chiavi crittografiche riservate e ogni altro dato personale come definito dalle leggi sulla protezione della *privacy*;
- registrarsi a siti i cui contenuti non siano connessi all'attività lavorativa;
- utilizzare sistemi di *chat*, *peer to peer*, *file sharing*, *podcasting*, *webcasting* e similari, oppure connettersi a siti che trasmettono *streaming* audio o video, senza essere preventivamente autorizzati dal *SIC*;
- scaricare software dalla rete senza essere preventivamente autorizzati dal *SIC*;

- utilizzare *provider* Internet diversi da quello ufficiale del Comune ed attivare connessioni diverse da quella centralizzata.

5. Posta Elettronica

L'utilizzo di posta elettronica è consentito solo per motivi istituzionali e connessi all'attività lavorativa, da parte di dipendenti ai quali è stata assegnata un'utenza di posta individuale o relativa all'ufficio o servizio.

In entrambi i casi, l'accesso è consentito in via esclusiva ai dipendenti ai quali sono state comunicate credenziali di autenticazione per l'accesso alla casella di posta.

In caso di necessità, l'utente può delegare un altro dipendente a verificare il contenuto dei messaggi.

L'utente deve avere consapevolezza che i contenuti della posta elettronica dell'ente non devono avere carattere privato o personale, ma devono riguardare esclusivamente questioni attinenti al lavoro dell'ufficio.

I messaggi di posta elettronica conterranno un avvertimento ai destinatari nel quale è dichiarata la natura non personale dei messaggi stessi e la precisazione che le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente.

E' vietato l'utilizzo di *client* di posta elettronica diversi da quello autorizzato ed installato come dotazione standard della postazione di lavoro. Esso dovrà essere configurato in modo da poter servire esclusivamente per la gestione di caselle di posta elettronica istituzionali (account del Comune), secondo i parametri di configurazione indicati.

All'utente di posta elettronica è vietato:

- trasmettere materiale commerciale e/o pubblicitario non richiesto (*spamming*), nonché permettere che le proprie risorse siano utilizzate da terzi per questa attività,
- utilizzare la posta elettronica per fini non connessi all'attività lavorativa (ad esempio giochi, scherzi, barzellette, appelli e simili), e con contenuti di carattere privato e personale,
- allegare ai messaggi materiale potenzialmente pericoloso (programmi, etc.) o di dimensioni eccessive, secondo le istruzioni ricevute,
- creare o trasmettere qualunque immagine, dato o altro materiale offensivo, diffamatorio, osceno, indecente, o che attenti alla dignità umana, specialmente se riguardante il sesso, la razza o il credo,
- eludere in qualsiasi modo i meccanismi di filtro *anti-spam* predisposti dall'ente, salvo far presente al *SIC* eventuali blocchi considerati non appropriati,
- installare o eseguire programmi, *scripts* o altro materiale eventualmente ricevuto come allegato senza autorizzazione del *SIC*.

6. Controlli previsti e sanzioni

Nel rispetto della normativa vigente, **l'ente *non procede* a verifiche che possano configurare il controllo a distanza dell'attività dei lavoratori**, quali:

- lettura e registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio *e-mail*;
- riproduzione ed eventuale memorizzazione sistematica delle pagine *web* visualizzate dal lavoratore;
- lettura e registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
- analisi occulta di computer portatili affidati in uso.

L'ente, peraltro, si riserva la facoltà di eseguire controlli in conformità alla legge, sia per eseguire verifiche sulla funzionalità e sicurezza di reti e sistemi, sia per eseguire verifiche sul corretto utilizzo dei servizi Internet e posta elettronica, in conformità a quanto prescritto dal presente disciplinare, dalla normativa posta a protezione dei dati personali e dal Documento Programmatico sulla Sicurezza vigente.

I controlli sono posti in essere dal *Responsabile della Sicurezza/Responsabile SIC*, formalmente nominato secondo il vigente DPS. Egli potrà avvalersi di personale esterno, appositamente nominato quale responsabile esterno di trattamento, secondo le previsioni del D. Lgs. 196/2003 e del vigente Documento Programmatico sulla Sicurezza.

Tali controlli sono eseguiti tenendo conto del *principio di graduazione* (par. 6.1 del Provvedimento del Garante per la Protezione dei Dati Personali 1/3/2007) e procederanno come segue:

a. In via preliminare l'ente provvederà ad eseguire dei controlli su dati aggregati e anonimi, riferiti all'intera struttura lavorativa ovvero a sue aree; tali controlli si concluderanno con un *avviso generalizzato* inerente all'eventualmente rilevato utilizzo anomalo degli strumenti aziendali; in assenza di successive anomalie non si effettueranno controlli su base individuale;
b. Nel perdurare delle anomalie si procederà a *controlli su base individuale* o per postazioni di lavoro;
c. In caso di abusi singoli e reiterati si procederà all'invio di *avvisi individuali* e si eseguiranno *controlli nominativi* o su singoli dispositivi e/o postazioni di lavoro;
d. In caso di riscontrato e reiterato uso non conforme delle risorse informatiche, il *Responsabile della Sicurezza/Responsabile SIC* segnalerà il comportamento al Titolare dei Trattamenti (Sindaco o Direttore Generale) e al responsabile della struttura di appartenenza del dipendente, il quale, trattandosi di violazione degli obblighi del dipendente, attiverà il *procedimento disciplinare* nelle forme e con le modalità previste dal C.C.N.L. e nel rispetto dei vigenti regolamenti dell'ente e delle vigenti disposizioni legislative in materia.

Per il personale dirigente il comportamento andrà segnalato al Titolare dei Trattamenti (Sindaco o Direttore Generale) e al competente Ufficio per i procedimenti disciplinari, per l'adozione degli atti di rispettiva competenza.

Per il personale non dipendente cui non è applicabile il C.C.N.L., il comportamento andrà segnalato al Titolare dei Trattamenti (Sindaco o Direttore Generale) e agli uffici competenti per l'adozione degli atti necessari.

7. Conservazione delle informazioni (tipo e durata)

Il servizio di accesso ad Internet produrrà delle registrazioni (*log*) conservate in forma elettronica per finalità di monitoraggio e controllo, fermi restando i divieti di cui al punto 6 (controllo a distanza).

I dati sono raccolti e archiviati in *forma anonima* e riguarderanno, per ciascun dominio/sito visitato, il numero di utenti che lo visitano, la quantità di dati scaricati, il numero di pagine richieste ed ogni eventuale ulteriore informazione di tipo statistico e quantitativo relativa alle modalità di utilizzo del servizio, con preclusione della raccolta e registrazione di informazioni riferite o riferibili a singoli utenti.

Tali dati potranno essere trattati per le seguenti finalità:

- richieste della Polizia delle Comunicazioni o dell'autorità giudiziaria,
- analisi e monitoraggio dell'utilizzo del servizio, con riferimento ad utilizzi anomali o in caso di eventi dannosi e situazioni di pericolo,
- statistiche relative all'utilizzo della rete.

Nel rispetto della procedura di controllo graduale definita al punto 6, è possibile, da parte del *Responsabile della Sicurezza/Responsabile SIC* o delle autorità competenti, approfondire l'analisi fino all'identificazione di attività riconducibili a singoli utenti.

I dati sono conservati per il tempo strettamente necessario al perseguimento delle finalità organizzative, produttive e di sicurezza e comunque *non oltre i sei mesi*; trascorso tale termine le registrazioni sono cancellate.

Sono raccolti e registrati, altresì, i dati relativi ai tentativi di accesso ai siti bloccati, al fine di segnalare agli utenti stessi eventuali reiterazioni dei tentativi e produrre avvisi individuali.

I dati sono conservati per il tempo strettamente necessario al perseguimento delle finalità organizzative, produttive e di sicurezza e comunque non oltre i sei mesi; trascorso tale termine le registrazioni sono cancellate.

Responsabile del trattamento dei dati di controllo è il *Responsabile della Sicurezza*, formalmente nominato secondo il vigente DPS. Egli potrà avvalersi di personale esterno, appositamente nominato quale responsabile esterno di trattamento, secondo le previsioni del D.Lgs. 196/2003 e del vigente Documento Programmatico sulla Sicurezza.