

# Comune di Siapiccia

Provincia di Oristano



## **DISCIPLINARE INTERNO PER L'UTILIZZO DI INTERNET E DELLA POSTA ELETTRONICA DA PARTE DEI DIPENDENTI**

Approvato con determinazione del Segretario – Direttore n. 95 del 05/08/2008

**Visto, il Rappr. Sindacale**

## Premessa

Dall'esame di diversi reclami, segnalazioni e quesiti pervenuti, il Garante per la protezione dei dati personali ha preso atto dell'esigenza di prescrivere ai datori di lavoro pubblici e privati alcune misure, necessarie o opportune, per conformare alle vigenti disposizioni in materia di Privacy il trattamento dei dati personali effettuato per verificare il corretto utilizzo, nel rapporto di lavoro, della Posta elettronica e di Internet. A tale scopo è stato emanato il Provvedimento generale pubblicato sulla Gazzetta Ufficiale della Repubblica Italiana – Serie generale n. 58 del 10/03/2007.

Il presente disciplinare, rivolto ai dipendenti del Comune di Siapiccia e a coloro che a vario titolo operano nelle strutture del Comune, fornisce concreto riscontro alle prescrizioni del Garante e si conforma a quanto previsto nelle conclusioni del Provvedimento, al punto 2), lett. a).

## Principi

Il presente disciplinare viene predisposto nel rispetto della vigente disciplina in materia di Privacy, con riguardo, in particolare, alle norme del D. Lgs. 196/2003 (Codice in materia di protezione dei dati personali) che disciplinano il trattamento effettuato dai soggetti pubblici. Il Comune di Siapiccia garantisce che il trattamento dei dati personali dei dipendenti, effettuato per verificare il corretto utilizzo della Posta elettronica e di Internet, si conforma ai seguenti principi:

1. Il principio di *necessità*, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite (art. 3 del Codice; par. 5.2 del Provvedimento);
2. Il principio di *correttezza*, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori (art. 11, c. 1, lett. a) del Codice) poiché le tecnologie dell'informazione, in modo più marcato rispetto ad apparecchiature tradizionali, permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa, anche all'insaputa o, comunque, senza la piena consapevolezza dei lavoratori (par. 3 del Provvedimento);
3. Il principio di *pertinenza e non eccedenza* (par. 6 del Provvedimento), in virtù del quale:
  - I trattamenti devono essere effettuati per finalità determinate, esplicite e legittime (art. 11, c. 1, lett. b) del Codice; par. 4 e 5 del Provvedimento);
  - Il datore di lavoro deve trattare i dati "nella misura meno invasiva possibile";
  - Le attività di monitoraggio devono essere svolte solo da soggetti preposti (par. 8 del Provvedimento) e essere mirate sull'area di rischio, tenendo conto della normativa in materia di protezione dei dati personali e, se pertinente, del principio di segretezza della corrispondenza (Parere n. 8/2001, punti 5 e 12).

## Definizioni

Nel presente documento il termine:

- **UTENTE INTERNET**: persona autorizzata ad accedere alla lista di siti istituzionali preventivamente selezionati dal Comune;
- **UTENTE DI POSTA ELETTRONICA**: persona autorizzata ad accedere al servizio di posta elettronica;
- **WHITE LIST**: elenco di siti direttamente e immediatamente accessibili da tutti gli utenti internet;
- **BLACK LIST**: elenco di siti non accessibili da nessun utente
- **INTERNET PROVIDER**: azienda che fornisce al Comune il canale di accesso alla rete internet;
- **POSTAZIONE DI LAVORO**: personal computer collegato alla rete comunale tramite il quale l'utente accede ai servizi;
- **LOG**: archivio delle attività di consultazione in rete;
- **RESPONSABILE DEL TRATTAMENTO**: responsabile ex articolo 29 del Codice in materia di protezione dei dati personali, D. Lgs. 196/2003.

### **Modalità di accesso e di utilizzo della postazione di lavoro**

La configurazione dei servizi di accesso a Internet e di Posta Elettronica viene eseguita esclusivamente dai tecnici del Servizio Informatica, che può essere affidato a Ditta esterna all'Amministrazione.

Le postazioni di lavoro sono preventivamente individuate e assegnate personalmente a ciascun dipendente; per accedere ai servizi informatici comunali dalla postazione di lavoro garantendone quindi la sua protezione, il dipendente dovrà utilizzare una password conforme alle prescrizioni contenute nel Documento Programmatico sulla Sicurezza adottato dal Comune. Superato il sistema di autenticazione, il dipendente sarà collegato alla rete comunale e ad internet senza formalità.

Il dipendente, preso atto che la conoscenza della password da parte di terzi consente a questi ultimi di accedere alla rete comunale nonché l'utilizzo dei relativi servizi in nome del titolare e l'accesso ai dati a cui egli stesso è abilitato, si impegna a:

1. Non cedere, una volta superata la fase di autenticazione, la propria postazione di lavoro a personale non autorizzato;
2. Non lasciare incustodita la propria postazione di lavoro una volta connessi al sistema;
3. Conservare la password nella massima riservatezza;
4. Non installare o non utilizzare programmi di sistema, applicativi o gestionali privi di regolare contratto di licenza d'uso sottoscritto dall'Ente, salvo specifica autorizzazione in tal senso da parte del Responsabile;
5. Non modificare le configurazioni (in modo particolare l'identificativo in rete del proprio Pc) impostato dall'Amministratore di sistema;
6. Non installare sul proprio Pc dispositivi hardware personali (modem, schede audio etc.), salvo specifica autorizzazione in tal senso da parte del Responsabile;
7. Mantenere il programma antivirus sempre attivo con riferimento all'ultima versione disponibile. In caso di impossibilità ad operare in tal senso è necessario fornire immediata segnalazione al proprio Responsabile;
8. Non utilizzare strumenti software e/o hardware atti ad intercettare il contenuto delle comunicazioni informatiche all'interno dell'Ente.

Per ciò che concerne l'utilizzo di supporti magnetici e ottici, il dipendente deve attenersi alle seguenti disposizioni:

1. Non è consentito scaricare files (programmi, archivi di dati, etc.) contenuti in supporti magnetici e/o ottici che non abbiano attinenza con la propria prestazione lavorativa;
2. E' fatto obbligo di sottoporre a controllo preventivo tutti i files di provenienza incerta o esterna, attinenti l'attività lavorativa;

### **Internet**

Tutti i dipendenti cui è assegnata dall'Amministrazione una postazione di lavoro possono utilizzare internet.

Il dipendente - 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.

Al dipendente non è consentito:

1. 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;
2. Effettuare transazioni finanziarie, operazioni di remote banking, acquisti on line e simili, se non attinenti l'attività lavorativa o direttamente autorizzati dal Responsabile;

3. Utilizzare sistemi Peer to Peer (P2P), di 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 dal Responsabile;
4. Scaricare software gratuiti (freeware, shareware, public domain etc.) dalla rete, salvo casi di comprovata utilità (es: antivirus) ed in ogni caso previa autorizzazione in tal senso da parte del Responsabile 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, facendo sì che venga installato da personale competente;
5. Utilizzare internet provider diversi da quello scelto ufficialmente dal Comune e la connessione di stazioni di lavoro aziendali alle reti di detti provider con sistemi di connessione diversi (es. modem) da quello centralizzato;
6. Registrarsi a siti i cui contenuti non siano attinenti con l'attività lavorativa;
7. Partecipare a forum e/o l'utilizzo di chat se non per motivi strettamente attinenti l'attività lavorativa;
8. Usare la rete in modo difforme da quanto previsto dal presente documento e dalle leggi penali, civili e amministrative in materia di disciplina dell'attività e dei servizi svolti sulla rete.

### **Posta elettronica**

L'utilizzo del servizio di posta elettronica è consentito solo per ragioni di servizio agli utenti identificati con le modalità precedentemente illustrate, ai quali l'amministrazione assegna una casella di posta per il proprio ufficio.

In caso di assenza l'utente può delegare un altro dipendente dell'ufficio a verificare il contenuto dei messaggi e ad inoltrare al datore di lavoro quelli ritenuti rilevanti e per lo svolgimento dell'attività lavorativa.

Al dipendente:

1. Non è consentito utilizzare la posta elettronica per motivi non attinenti allo svolgimento delle mansioni assegnate;
2. Non è consentito l'utilizzo dell'indirizzo di posta elettronica istituzionale per la partecipazione a dibattiti, forum e mail-list, salvo specifica autorizzazione in tal senso da parte del Responsabile;
3. E' sconsigliato e quindi da evitare l'apertura di allegati di non comprovata origine in assenza di software antivirus aggiornati sulla propria postazione di lavoro;
4. E' sconsigliato e quindi da evitare la chiamata a link contenuti all'interno di messaggi a meno di comprovata sicurezza sul contenuto dei siti richiamati;
5. E' sconsigliato e quindi da evitare il download di file con estensioni: .vbs, .bat, .exe o file e successiva esecuzione delle macro in esso contenute;
6. E' sconsigliato e quindi da evitare la risposta ad e-mail pervenute da mittenti sconosciuti. Si suggerisce, nel dubbio, di cancellarle preventivamente;
7. E' sconsigliato l'invio di allegati in formato Ms-Word (estensione .doc): utilizzare in alternativa il formato RTF (estensione .rtf);
8. E' sconsigliato l'invio e l'accettazione anche in sola lettura di messaggi formato html;
9. E' vietato utilizzare tecniche di "mail spamming" cioè di invio massiccio di comunicazioni a liste di distribuzione extra aziendali o di azioni equivalenti;
10. E' vietato utilizzare il servizio di posta elettronica per inoltrare giochi, scherzi, barzellette, appelli e petizioni (anche se possono sembrare veritieri e socialmente utili), messaggi tipo "catene di S. Antonio" e altre e-mails che non siano di lavoro;
11. E' vietato allegare al testo delle comunicazioni materiale potenzialmente insicuro (ad es. programmi, scripts, macro), così come file di dimensioni eccessive.

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.

## Controlli

L'Amministrazione, 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 dell'art. 4, comma due dello Statuto dei Lavoratori, di sistemi che consentano indirettamente un controllo a distanza (cd. controllo preterintenzionale), e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori, nel rispetto di quanto previsto dal paragrafo 5 del Provvedimento.

L'amministrazione non effettua in alcun caso trattamenti di dati personali mediante sistemi hardware e software che mirano al controllo a distanza dei lavoratori grazie ai quali sia possibile ricostruire la loro attività e che vengano svolte tramite i seguenti mezzi:

- ❑ Lettura e registrazione sistematica dei messaggi di posta elettronica dei dipendenti ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per fornire il servizio di posta elettronica;
- ❑ Riproduzione e eventuale memorizzazione sistematica delle pagine web visualizzate dal dipendente;
- ❑ Lettura e registrazione dei caratteri inseriti dai lavoratori tramite la tastiera ovvero dispositivi analoghi a quello descritto;
- ❑ Analisi occulta dei dispositivi per l'accesso a Internet o l'uso della posta elettronica messi a disposizione dei dipendenti.

Le attività sull'uso del servizio di accesso ad internet vengono automaticamente registrate in forma elettronica attraverso i LOG di sistema.

Il trattamento dei dati contenuti nei LOG può 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 del Segretario Comunale - Direttore per le valutazioni di competenza e riguardano:

- ❑ per ciascun sito/dominio visitato le seguenti informazioni: il numero di utenti che lo visitano, il numero delle relative pagine richieste e della quantità di dati scaricati;
- ❑ per ciascun utente le seguenti informazioni: il numero di siti visitati, la quantità totale di dati scaricati, e le postazioni di lavoro utilizzate per la navigazione.

I dati personali contenuti nei log possono 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 Segretario Comunale - Direttore quando si verifichi un evento dannoso o una situazione di pericolo che richieda un immediato intervento;
- ❑ su richiesta del Segretario Comunale - Direttore 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 Segretario Comunale - Direttore ad attenersi ai compiti assegnati ed alle istruzioni impartite.

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 6 mesi, e sono periodicamente cancellati automaticamente dal sistema.

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.

### **Entrata in vigore e aggiornamento**

Il presente disciplinare verrà pubblicato all'Albo Pretorio del Comune e verrà trasmesso a ciascun dipendente. Esso entrerà in vigore a partire dal 15° giorno successivo alla pubblicazione nell'albo pretorio del Comune.

Il presente disciplinare viene sottoposto a revisione, solo se oggetto di variazioni, in sede di aggiornamento del Documento Programmatico sulla sicurezza di cui al D. Lgs. 196/2003, art. 33.