CITTÀ DI MONCALIERI
Settore Servizi Demografici e CED
Servizio Informatico
Tel. 011/6401 386 - fax 011/64 12 46 - e-mail: segreteria.sed@comune.moncalieri.to.it

Policy dell'Ente a norma di Regolamento per l'utilizzo degli strumenti informatici e telematici.

INDICE

File	Vers.	Emesso da:	data:
reg_utilizzo_strumenti_inform_telematici_sett2008.doc	1.0	Fabrizio Rodano	13/11/13

1. PREMESSA.

Oggi l'utilizzo massiccio di strumenti informatici nell'attività lavorativa, compreso Internet e la posta elettronica, sempre più ci espongono a problemi di sicurezza aziendale.

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche del nostro Comune deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, la presente nota è diretta ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati.

Tali note si aggiungono alla deliberazione di Giunta Comunale N. 120/2000 ("Misure di sicurezza per la protezione dei dati personali – Approvazione del Documento Programmatico – Piano Operativo di Intervento") ed integrano le specifiche istruzioni già fornite a tutti gli incaricati al trattamento dei dati personali e sensibili (con determinazione specifica di ogni dirigente), in attuazione del Decreto Legislativo 30 giugno 2003, n. 196 ("Codice in materia di protezione dei dati personali") e del Decreto del Presidente della Repubblica 28 luglio 1999, n. 318 ("Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali…").

2. UTILIZZO DEL PERSONAL COMPUTER.

1) Il Personal Computer e le periferiche affidate al dipendente sono uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

2) L'accesso alla rete comunale dalla stazione di lavoro è protetto da parola chiave, formata e gestita ai sensi dell'Allegato B del Decreto Legislativo 30 giugno 2003, n. 196, che deve essere custodita con diligenza dal lavoratore e per nessun motivo divulgata a terzi. L'accesso al BIOS della macchina è consentito solo agli Amministratori di Sistema.

3) Gli Amministratori di Sistema, esclusivamente per l'espletamento delle loro funzioni, hanno la facoltà in qualunque momento di accedere ai dati trattati da ciascuno.

   Per esigenze di carattere produttivo e di sicurezza dei dati e delle postazioni di lavoro, il Servizio Informatico potrà installare sulle postazioni di lavoro ed attivare software per

l'assistenza remota da utilizzarsi esclusivamente per risolvere problematiche hardware e software a fronte di una chiamata di assistenza da parte del lavoratore.

In nessun caso tali strumenti consentono un controllo a distanza dell'operato del lavoratore, prefigurando in tal caso profili di tipo disciplinare per gli Amministratori di Sistema.

4) Non è consentito installare autonomamente programmi provenienti dall'esterno salvo preventiva ed esplicita autorizzazione degli Amministratori di Sistema. Colui che ha installato abusivamente programmi provenienti dall'esterno risponde direttamente dei danni eventualmente arrecati. In tal caso non si garantisce il ripristino delle funzionalità della stazione di lavoro.

5) Non è consentito l'uso di programmi diversi da quelli distribuiti dal Servizio Informatico del Comune di Moncalieri e per i quali si applicano le norme sui diritti d'autore (Decreto Legislativo 29 dicembre 1992, n. 518 sulla tutela giuridica dei programmi per elaboratore come modificato dal Decreto Legislativo 15 marzo 1996, n. 205, Legge 18 agosto 2000, n. 248 sulle nuove norme di tutela del diritto d'autore, Decreto Legislativo 9 aprile 2003, n. 68).

6) Non è consentito all'utente modificare le caratteristiche impostate sul proprio Personal Computer, salvo preventiva ed esplicita autorizzazione degli Amministratori di Sistema.

7) Il Personal Computer deve essere spento ogni sera al termine della giornata lavorativa ed in caso di assenze prolungate dall'ufficio. In ogni caso lasciare la postazione di lavoro incustodita e connessa alla rete aziendale può configurare un principio di comportamento non diligente e corretto, in caso di utilizzo di terzi fraudolento.

8) Non è consentita l'installazione sul proprio PC di nessun dispositivo hardware di vario genere (per esempio, masterizzatori, pen drive, …), se non con l'autorizzazione esplicita degli Amministratori di Sistema. Non è consentito lo spostamento fisico di PC e periferiche, senza previa autorizzazione degli Amministratori di Sistema.

9) Il Servizio Informatico potrà attivare controlli a campione su postazioni di lavoro di ciascuna Area organizzativa per verificare se vi sono presenti componenti hardware e/o software non autorizzati. In tal caso se ne procederà alla disinstallazione e/o rimozione ed a mettere in atto i provvedimenti di cui al punto 11 del presente Disciplinare. Gli Amministratori di Sistema sono tenuti ad informare il Responsabile del trattamento dati dell'Area organizzativa interessata, il quale può disporre verifiche più approfondite, tramite gli Amministratori di Sistema, allo scopo di mettere in evidenza eventuali condotte illecite del lavoratore stesso, che daranno luogo a rilievo disciplinare.

10) Agli utenti incaricati del trattamento dei dati sensibili e giudiziari è vietato l'accesso contemporaneo con lo stesso identificativo da più Personal Computer (art. 5 del Decreto del Presidente della Repubblica 28 luglio 1999, n. 318).

11) Ogni utente deve prestare la massima attenzione ai supporti di origine esterna (floppy disk, CD-R, …), avvertendo immediatamente gli Amministratori di Sistema nel caso in cui siano rilevati

virus ed adottando quanto previsto dal successivo punto 8 della presente nota relativo alle procedure di protezione antivirus.

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

3. UTILIZZO DELLA RETE COMUNALE.

1. Le unità di rete (server di rete, di posta e di database) sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità, vengono svolte regolari attività di controllo, amministrazione e backup giornaliero da parte degli Amministratori di Sistema
2. Gli Amministratori di Sistema possono in qualunque momento procedere alla rimozione di ogni file o applicazione ritenuti pericolosi per la Sicurezza sia sui Personal Computer degli incaricati sia sulle unità di rete.
3. Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi di rete, con cancellazione dei file obsoleti o inutili.
4. E' cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni.
5. Per quanto riguarda la presenza di *modem e/o router* per collegamenti remoti o di teleassistenza, è necessario che i suddetti vengano accesi solo durante l'utilizzo del relativo servizio ed al termine immediatamente spenti, al fine di evitare intromissioni fraudolente sulla rete comunale.

4. GESTIONE DELLE PASSWORD.

4.1 Password rilasciate a protezione di ciascuna stazione di lavoro:

- PC ASSEGNATI ALL'UFFICIO: il BIOS di tali macchine è protetto da password specifica conosciuta esclusivamente dagli Amministratori di Sistema.

4.2 Password rilasciate per accedere alle funzionalità applicative dei sistemi centrali o dipartimentali, nei limiti stabiliti dal profilo e codice identificativo correlato:

- FUNZIONALITA' DISPONIBILI IN RETE LOCALE: si accede alla rete locale mediante password scelta dall'incaricato, nota a lui solo; la password scade automaticamente ogni 90 giorni ed è rinnovabile autonomamente a cura dell'incaricato; non deve essere divulgata; autorizza all'utilizzo delle funzionalità connesse al profilo e al codice identificativo attribuito dagli amministratore di rete incaricati. In assenza di tale password non è possibile accedere alla postazione di lavoro.

- FUNZIONALITA' DI POSTA ELETTRONICA: sono accessibili mediante password scelta dall'incaricato, non divulgabile, modificabile ogni 180 giorni a propria cura;

- FUNZIONALITA' GESTIONALI SISTEMI CENTRALI: GESTIONE DOCUMENTALE / BILANCIO / DEMOGRAFICI / VERBALI / SW GESTIONE MENSE: sono accessibili mediante pw assegnate dagli Amministratori di Sistema; dette password, da non divulgare, sono generalmente modificabili ogni 180 mesi a cura dell'incaricato del trattamento dei dati.

5. ACCESSO ED UTILIZZO DEGLI ARCHIVI ELETTRONICI.

1. I supporti informatici contenenti file con dati sensibili vengono conservati separatamente in armadi e contenitori muniti di serratura e sono resi accessibili unicamente agli incaricati al trattamento degli stessi
2. Al termine delle eventuali operazioni di trattamento dati, i suddetti supporti devono essere riposti nei relativi armadi e contenitori.
3. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili,ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

6. UTILIZZO DI PC PORTATILI (NOTEBOOK).

1. L'utente è responsabile del PC portatile assegnatogli dagli Amministratori di Sistema e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
2. Ai PC portatili, utilizzati in ambito aziendale, si applicano le regole di utilizzo previste per i PC connessi in rete.

3. Non è consentito in nessuna maniera, per ragioni di sicurezza, l'utilizzo di PC portatili di proprietà dell'utente sulla rete aziendale.

7. UTILIZZO DELLA POSTA ELETTRONICA.

1. La casella di posta, assegnata dal Comune all'utente, è principalmente uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

2. E' buona norma utilizzare la casella di posta specifica per ogni ufficio/servizio (del tipo ufficio@... o segreteria.ufficio@...) per lo scambio di messaggi di tipo istituzionale o con altre amministrazioni. E' possibile affiancare le caselle di posta condivise per ufficio a quelle individuali.

3. E' vietato inoltrare a tutti gli utenti interni di posta elettronica messaggi di tipo strettamente personale, per nulla attinenti l'attività lavorativa.

4. E' buona norma evitare messaggi completamente estranei al rapporto di lavoro od iscrizioni a mailing list inutili. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

5. E' possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario. Tale ricevuta, non essendo legata a caselle di posta elettronica certificata dell'Ente, potrà arrivare solo se è opportunamente configurato il server di posta elettronica del destinatario del messaggio.

6. In caso di assenza programmata dall'ufficio (per esempio per ferie od attività di lavoro fuori sede), il lavoratore deve attivare la voce "Assenza ufficio" dal proprio client di posta elettronica, impostando un messaggio comprensivo delle coordinate (anche elettroniche e/o telefoniche) di altro soggetto della struttura da contattare nel medesimo periodo d'assenza. Se il lavoratore, per assenza improvvisa, non può attivare tale procedura, il Titolare del trattamento, tramite i Responsabili del trattamento dei dati nominati ai sensi del Decreto Legislativo 30 giugno 2003, n. 196, può disporre lecitamente l'attivazione di analogo accorgimento mediante gli Amministratori di Sistema.

7. Qualora si debba conoscere il contenuto di messaggi di posta elettronica di un lavoratore in assenza improvvisa o prolungata per inderogabili necessità legate all'attività lavorativa, il lavoratore deve delegare un altro lavoratore fiduciario a verificare il contenuto dei messaggi ed ad inoltrare ai Responsabili del trattamento quelli ritenuti rilevanti per l'attività lavorativa. In caso d'impedimento dell'interessato, procede il Responsabile del trattamento tramite gli Amministratori di Sistema. Di tale attività, a cura del Responsabile del trattamento, viene redatto apposito verbale ed informato il lavoratore stesso alla prima occasione utile.

8. Il sistema di posta elettronica, se tecnicamente possibile, inserisce un messaggio che precisa che ogni eventuale opinione personale espressa è dell'autore e dunque non costituisce alcun impegno contrattuale fra l'Ente ed il destinatario. L'Ente inoltre non assume alcuna responsabilità riguardo al contenuto del testo e dei relativi allegati, né per eventuali intercettazioni, modifiche o danneggiamenti al messaggio originale.

9. E' obbligatorio controllare i file allegati a messaggi di posta elettronica prima del loro utilizzo. Non lanciare mai in esecuzione o provare ad aprire file allegati di tipo o nome sconosciuto o poco chiaro.

10. E' vietato inviare catene telematiche (o di Sant'Antonio). Se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente agli Amministratori di Sistema.

11. Presso il Servizio Informatico vengono conservati i file di log della posta elettronica esclusivamente per ragioni di sicurezza, verifiche, accertamento e repressione di reati a disposizione esclusiva delle autorità giudiziaria e di polizia, per un periodo non superiore a due (due) mesi. Sono inoltre conservate per un periodo non superiore a 2 (due) mesi copie di backup delle caselle di posta elettronica, utilizzabili esclusivamente per ripristini di dette caselle dovute a corruzioni dei database di posta, a cancellazioni errate di e-mail da parte del lavoratore o a ricostruzioni in caso di grave avaria del sistema servente.

12. Saranno attivabili controlli a campione sui log della posta elettronica atti a verificare l'eventuale flusso anomalo di messaggi di posta in uscita dall'Ente. In tal caso gli Amministratori di Sistema sono tenuti ad informare il Responsabile del trattamento dati dell'Area organizzativa interessata, il quale può disporre verifiche più approfondite, tramite gli Amministratori di Sistema, allo scopo di mettere in evidenza eventuali condotte illecite del lavoratore, quali invio di informazioni e/o dati consistente in un concreto pericolo di pregiudizio al patrimonio dell'Ente o violazione dei vincoli di riservatezza e sicurezza a cui il lavoratore è tenuto sul posto di lavoro. Se viene accertata la condotta illecita da parte del lavoratore, gli Amministratori di Sistema ne danno segnalazione in forma scritta al Responsabile del trattamento dei dati. Dalla data di tale segnalazione decorrono i tempi di cui all'art. 24 del Contratto Nazionale Collettivo comparto Enti Locali del 22 gennaio 2004.

8. UTILIZZO DI INTERNET E DEI RELATIVI SERVIZI.

1. Il PC abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. E' assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa e su siti non pertinenti all'attività lavorativa (quali ad esempio siti d'intrattenimento,…). Presso il Servizio Informatico comunale sono attivati sistemi di "filtraggio" dei contenuti e pagine Web che bloccano o quantomeno limitano la navigazione su siti illegali o per categorie di siti ben specifiche che

siano illegali per la legge italiana (quali pedofilia, gioco d'azzardo, ecc.) o comunque ledenti la dignità umana (violenza, razzismo, …).

2. E' fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, di file musicali e video di qualsiasi genere scaricati dalla Rete o tramite software di tipo "peer to peer". Il download di software dalla rete Internet deve essere espressamente autorizzato dagli Amministratori di Sistema.

3. E' da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.

4. E' vietata categoricamente la partecipazione a forum non professionali, l'iscrizione a newsgroup non attinenti l'attività lavorativa e l'utilizzo di chat line.

5. Presso il Servizio Informatico sono attivi strumenti statistici e di monitoraggio che rilevano i siti più visitati, fornendo dati in forma aggregata e in nessuna maniera riconducibili al singolo individuo.

6. Periodicamente e previa comunicazione ai lavoratori ed alle rappresentanze sindacali potranno essere attivati verifiche su tali dati di navigazione in forma anonima ed aggregata. Tali verifiche si potranno concludere con un avviso generalizzato relativo ad un rilevato utilizzo anomalo della navigazione Internet e con l'invito ad attenersi scrupolosamente alle disposizioni del presente Regolamento.

7. Presso il Servizio Informatico vengono conservati i file di log della navigazione Internet esclusivamente per ragioni di sicurezza e verifiche a disposizione esclusiva delle autorità giudiziaria e di polizia, per un periodo non superiore a 2 (due) mesi.

8. I servizi di Voice Over IP (VOIP) già utilizzati e che verranno progressivamente ampliati all'interno dell'Ente sono soggetti alle restrizioni del presente paragrafo, trattandosi di servizi che utilizzando la banda Internet.

9. Saranno attivabili controlli a campione sui log della navigazione Internet atti a verificare l'eventuale occupazione anomala della banda Internet in uscita dall'Ente. In tal caso gli Amministratori di Sistema sono tenuti ad informare il Responsabile del trattamento dati dell'Area organizzativa interessata, il quale può disporre verifiche più approfondite, tramite gli Amministratori di Sistema, allo scopo di mettere in evidenza eventuali condotte illecite del lavoratore, quali invio di informazioni e/o dati consistente in un concreto pericolo di pregiudizio al patrimonio dell'Ente o violazione dei vincoli di riservatezza e sicurezza a cui il lavoratore è tenuto sul posto di lavoro. Se viene accertata la condotta illecita da parte del lavoratore, gli Amministratori di Sistema ne danno segnalazione in forma scritta al Responsabile del trattamento dei dati. Dalla data di tale segnalazione decorrono i tempi di cui all'art. 24 del Contratto Nazionale Collettivo comparto Enti Locali del 22 gennaio 2004.

9. PROTEZIONE ANTIVIRUS.

1. Gli incaricati sono tenuti a verificare che i PC in dotazione siano costantemente sottoposti a controllo anti-virus e ad accertarsi che il software anti-virus venga aggiornato almeno due volte al mese, evidenziandone tempestivamente le carenze eventuali e le sospette infezioni da virus al referente informatico o agli Amministratori di Sistema presso il Servizio Informatico.

10. OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY.

1. Le disposizioni in materia di Protezione dei dati personali e di misure minime di sicurezza sono contenute nel Regolamento Comunale approvato con deliberazione del Consiglio Comunale 01/02/2001 n. 7/2001, nella deliberazione della Giunta Comunale 29/03/2000, n. 120/2000, negli atti d'incarico dei Responsabili del trattamento dei dati, nel Decreto Legislativo 30 giugno 2003, n. 196, nel Decreto del Presidente della Repubblica 28 luglio 1999, n. 318, e nel Documento Programmatico per la Sicurezza dell'Ente, approvato annualmente con Delibera di Giunta con le relative modificazioni annuali.

11. INOSSERVANZA DELLE DISPOSIZIONI DEL REGOLAMENTO.

1. Si rimanda alle disposizioni degli articoli del Titolo IV del Contratto Nazionale Collettivo comparto Enti Locali del 22 gennaio 2004 ed al Codice di comportamento dei dipendenti delle pubbliche amministrazioni in allegato a detto Contratto Nazionale Collettivo.
2. Restano comunque applicabili le sanzioni penali, amministrative o contabili, previste da altre disposizioni.

12. DISPOSIZIONE FINALE.

1. Del presente atto viene data conoscenza a tutti i lavoratori interessati, mediante pubblicazione sulla Intranet aziendale, affissione alle bacheche di informazione per i lavoratori ed attraverso invio via e-mail a ciascun lavoratore, che potrà poi procedere autonomamente a stampa di copia cartacea.

13. AGGIORNAMENTO E REVISIONE.

1. Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento.

2. Il presente Regolamento è soggetto a revisione con frequenza biennale.

14. RIFERIMENTI NORMATIVI.

- Legge 20 maggio 1970, n. 300, "Statuto dei lavoratori"

- Decreto del Presidente della Repubblica 28 luglio 1999, n. 318 ("Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali…")

- Deliberazione di Giunta Comunale N. 120/2000 ("Misure di sicurezza per la protezione dei dati personali – Approvazione del Documento Programmatico – Piano Operativo di Intervento")

- Deliberazioni di Giunta comunale annuali di approvazione degli aggiornamenti del Documento Programmatico sulla Sicurezza (DPS)

- Decreto Legislativo 30 giugno 2003, n. 196 ("Codice in materia di protezione dei dati personali")

- Garante per la Protezione dei dati personali – "Linee guida per posta elettronica ed Internet" approvate il 1° marzo 2007 e pubblicate in Gazzetta Ufficiale n. 58 del 10 marzo 2007

- Garante per la Protezione dei dati personali – "Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico" del 14 giugno 2007 e pubblicate in Gazzetta Ufficiale n. 161 del 13 luglio 2007

- Decreto Legislativo 29 dicembre 1992, n. 518 sulla tutela giuridica dei programmi per elaboratore come modificato dal Decreto Legislativo 15 marzo 1996, n. 205

- Legge 22 aprile 1941, n. 633 e successive modificazioni: "Protezione del diritto d'autore e di altri diritti connessi al suo esercizio"

- Legge 18 agosto 2000, n. 248 sulle nuove norme di tutela del diritto d'autore

- Decreto Legislativo 9 aprile 2003, n. 68

- ISO/IEC JTC 1 17799:2005 "Information technology - Security techniques - Code of practice for information security management."