COMUNE DI CARATE BRIANZA

PROVINCIA DI MILANO

REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI

Approvato con Deliberazione di Giunta Comunale n. 261 del 10.12.2007

Premessa

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet dai Personal Computer, espone il Comune di Carate Brianza ai rischi di un coinvolgimento sia patrimoniale sia penale, creando problemi alla sicurezza e all'immagine dell'Ente stesso.
Premesso quindi che l'utilizzo delle risorse informatiche e telematiche del nostro Ente deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, il Comune ha adottato un Regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati.

Art. 1 Utilizzo del Personal Computer

Il Personal Computer affidato al dipendente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.
L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata. La stessa password permette l'accesso alla rete, ad internet, e deve essere attivata per lo screen saver.
Non è consentito installare autonomamente programmi provenienti dall'esterno salvo previa autorizzazione esplicita del Responsabile dei sistemi informatici, in quanto sussiste il grave pericolo di portare virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.
Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dal responsabile dei sistemi informatici del Comune di Carate Brianza.
L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'Ente a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software (D. Lgs. 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore) che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore.
Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze

prolungate dall'ufficio. In ogni caso 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. In ogni caso deve essere attivato lo screen saver e la relativa password.
Non è consentita l'installazione sul proprio PC di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, …), se non con l'autorizzazione espressa del Responsabile dei sistemi informatici. Ogni utente deve prestare la massima attenzione ai supporti di origine esterna.

2. Utilizzo della rete del Comune di Carate Brianza

Le unità di rete 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.

È assolutamente proibito entrare nella rete e nei programmi con altri nomi utente.
Il Responsabile dei sistemi informatici può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.
Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante.

3. Utilizzo delle stampanti di rete

È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni. È buona regola evitare di stampare documenti o file non adatti (per motivi di privacy) su stampanti comuni. In caso di necessità la stampa in corso può essere cancellata.

4. Gestione delle Password

Le password di ingresso alla rete, di accesso ai programmi e dello screen saver, sono previste ed attribuite dal Responsabile dei sistemi informatici.
È necessario procedere alla modifica della password a cura dell'incaricato del trattamento al primo utilizzo e, successivamente, almeno ogni sei mesi; nel caso di trattamento di dati sensibili e di dati giudiziari la periodicità della variazione deve essere ridotta a tre mesi.
Le password possono essere formate da lettere (maiuscole o minuscole) e numeri ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema; devono essere composte da almeno otto caratteri e non devono contenere riferimenti agevolmente riconducibili all'incaricato.
La password deve essere immediatamente sostituita, dandone comunicazione al Responsabile dei Sistemi Informatici, nel caso si sospetti che la stessa abbia perso la segretezza.

5. Utilizzo dei supporti magnetici

Tutti i supporti magnetici riutilizzabili (dischetti, cassette, cartucce) contenenti dati sensibili e giudiziari devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato. Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione. In caso di dismissione, questi supporti dovranno essere distrutti a cura dell'incaricato del trattamento.

I supporti magnetici contenenti dati sensibili e giudiziari devono essere custoditi in armadi ignifughi chiusi a chiave o in cassaforte.

6. Utilizzo di Personal Computer portatili

L'utente è responsabile del Personal Computer portatile assegnatogli da Responsabile dei sistemi informatici e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
Ai PC portatili si applicano le regole di utilizzo previste per i PC connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.
I PC portatili utilizzati all'esterno (convegni, fiere, ecc…), in caso di allontanamento, devono essere custoditi in un luogo protetto.

7. Uso della posta elettronica

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

È fatto divieto di utilizzare le caselle di posta elettronica dell'Ente…@comune.caratebrianza.mi.it per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list salvo diversa ed esplicita autorizzazione.
È buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi.
La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.
Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per il Comune di Carate Brianza deve essere visionata od autorizzata dal responsabile di settore, o, in ogni modo è opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria.
La documentazione elettronica che costituisce per l'Ente "know how" tecnico protetto (tutelato in base all'art. 6 bis del r.d. 29.6.1939 n.1127), e che, quindi, viene contraddistinta da diciture od avvertenze dirette ad evidenziarne il carattere riservato o segreto a tutela del patrimonio dell'Ente, non può essere comunicata all'esterno senza preventiva autorizzazione del responsabile di settore.
Per la trasmissione di file all'interno del Comune di Carate Brianza è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati.
È obbligatorio controllare i file attachements di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).
È vietato inviare catene telematiche. Se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al Responsabile dei sistemi informatici. Non si devono in alcun caso attivare gli allegati di tali messaggi.

8. Uso della rete Internet e dei relativi servizi

Il Personal Computer abilitato alla navigazione in Internet costituisce uno strumento necessario allo svolgimento della propria attività lavorativa. È assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.
E' fatto divieto all'utente lo scarico e comunque l'installazione di software prelevato da siti Internet o da altre fonti, se non espressamente autorizzato dal Responsabile dei sistemi informatici.

È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dai responsabili di settore e con il rispetto delle normali procedure di acquisto.
È da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.
È vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).
Il responsabile dei servizi informatici, anche su richiesta dei Responsabili di settore, può configurare sistemi che impediscano a tutti o ad alcune categorie di dipendenti, l'accesso a determinati siti e il download di files o software.

9. Osservanza delle disposizioni in materia di Privacy

È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, come indicate nella lettera di designazione di incaricato del trattamento dei dati ai sensi del disciplinare tecnico allegato al D.lgs.vo n. 196/2003, e nel Documento Programmatico per la Sicurezza, approvato dalla Giunta Comunale.

10. Controlli

L'Amministrazione comunale si riserva di effettuare controlli sull'utilizzo di internet e della posta elettronica da parte dei dipendenti.
A tal fine, in ottemperanza al Provvedimento n.13 del 1.3.2007 del Garante della Privacy, il Responsabile dei Sistemi informativi può effettuare controlli generalizzati a livello di settore o di ufficio.
Il controllo anonimo può concludersi con un avviso, circoscritto ai dipendenti del settore o ufficio interessato, relativo ad un rilevato utilizzo anomalo degli strumenti informatici e con l'invito ad attenersi alle istruzioni impartite.
Solo nel caso di mancata ottemperanza all'invito è lecito effettuare controlli su singoli dipendenti.
In ogni caso non sono ammessi controlli a distanza dei lavoratori, né la lettura e la registrazione dei messaggi di posta elettronica ovvero dei relativi dati esteriori, aldilà di quanto tecnicamente necessario per svolgere il servizio e-mail.

11. Procedura da adottare in caso di assenza prolungata

In caso di assenza prolungata del dipendente (maternità, malattia, infortunio etc), il responsabile dei sistemi informatici provvede alla attribuzione di una nuova password al sostituto. Al rientro del dipendente sostituito, questa password sarà disattivata.

12. Non osservanza della normativa dell'Ente

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

13. Aggiornamento e revisione

Il presente Regolamento è soggetto a revisione in caso di necessità.