Comune di Bracciano

Regolamento per l’utilizzo degli strumenti e dei servizi informatici e telematici dell’ente

Regolamento per l’utilizzo degli strumenti e dei servizi informatici e telematici dell’ente

(Approvato con deliberazione di C.C. n. 58 del 27.09.2010)

Indice

Art. 1 - Premessa

1.1 La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet da parte dei Personal Computer da un lato ha consentito l'introduzione di innovative tecniche di gestione, dall'altro ha dato origine a numerose problematiche relative all'utilizzo degli strumenti informatici forniti al dipendente per lo svolgimento delle proprie mansioni. In questo senso, è fortemente sentita dall'Amministrazione la necessità di porre in essere adeguati sistemi di controllo sull'utilizzo di tali strumenti da parte dei dipendenti e di sanzionare conseguentemente quegli usi scorretti che, oltre ad esporre l'Ente stesso a rischi tanto patrimoniali quanto penali, possono di per sé considerarsi contrari ai doveri di diligenza e fedeltà. I controlli preventivi e continui sull'uso degli strumenti informatici devono garantire tanto il diritto dell'Amministrazione di proteggere l'Ente, essendo i computer strumenti di lavoro la cui utilizzazione personale è preclusa, quanto il diritto del lavoratore a non vedere invasa la propria sfera personale, e quindi il diritto alla riservatezza ed alla dignità come sanciti dallo Statuto dei lavoratori e dal D.lgs 196/03 sulla tutela dei dati personali.

Art. 2 - Oggetto

2.1 Il Regolamento Comunale, di seguito riportato, disciplina le condizioni per il corretto utilizzo degli strumenti e dei servizi informatici, in particolare alla luce degli obblighi previsti dal D.lgs 196/2003 (Codice in materia di protezione dei dati personali), nonché gli obblighi previsti dal Disciplinare tecnico sulle misure minime di sicurezza allegato allo stesso Codice e dalle Linee guida emanate dall'Autorità Garante per la protezione dei dati personali, con propria deliberazione n. 13 del 1 marzo 2007, sulla disciplina della navigazione in internet e sulla gestione della posta elettronica nei luoghi di lavoro.

Art. 3 - Campo di applicazione del regolamento

3.1 Il Regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori dell'Ente a prescindere dal rapporto contrattuale intrattenuto con lo stesso (lavoratori somministrati, collaboratore a progetto, in stage, etc.).

3.2 Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche, per "utente" deve intendersi ogni dipendente e collaboratore (collaboratore a progetto, in stage, agente, etc.) in possesso di specifiche credenziali di autenticazione. Tale figura potrà anche venir indicata quale "incaricato del trattamento".

Art. 4 - Utilizzo del Personal Computer

4.1 Il Personal Computer affidato all'utente 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. Il personale deve custodire la propria strumentazione in modo appropriato e diligente, segnalando tempestivamente ogni danneggiamento, furto o smarrimento al proprio responsabile di servizio.

4.2 L'accesso al Personal Computer è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata. Le password devono essere utilizzate per l'accesso alla rete, per l'accesso a qualsiasi applicazione che lo preveda e per lo screen saver.

4.3 l'Amministratore di Sistema (d'ora innanzi Ads) e lo staff da lui diretto, per l'espletamento delle funzioni e mansioni assegnate, ha la facoltà di compiere interventi nel sistema informatico comunale diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware etc.) di monitorare lo spazio occupato dalle caselle di posta elettronica sul

server e informare gli utenti circa l'opportunità di liberare spazio, cancellando alcuni messaggi, quando lo spazio libero si approssima a zero.
Tali interventi potranno anche comportare l'accesso, in qualunque momento, ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, nonché alla verifica sui siti internet acceduti dagli utenti abilitati alla navigazione esterna. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'Ente, si applica anche in caso di assenza prolungata od impedimento dell'utente.

4.4 L'AdS ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni Personal Computer al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento viene effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, verrà data comunicazione all'utente assente o impedito, stendendo apposito verbale, in cui verranno spiegate modalità e motivazioni dell'intervento stesso.

4.5 Non è consentito l'uso di programmi diversi da quelli distribuiti ufficialmente dai Sistemi Informativi né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno senza la preventiva autorizzazione dell'Amministratore di sistema ed una richiesta scritta da parte del dirigente responsabile dell'unità cui è assegnato il Personal Computer. In caso di necessità di acquisto o dotazione di software applicativi e/o procedure pertinenti esclusivamente alcune aree deve essere richiesta per iscritto l'autorizzazione preventiva del Amministratore di Sistema, per garantire la compatibilità funzionale, tecnica ed il mantenimento dell'efficienza operativa dei sistemi e delle reti. Sussiste infatti il grave pericolo di introdurre involontariamente virus informatici o di alterare la stabilità delle applicazioni degli elaboratori e dei sistemi operativi.

4.6. E' vietato copiare o mettere a disposizione di altri utenti materiale protetto dalla legge sul diritto d'autore (documenti, file musicali, immagini, filmati e simili) di cui l'ente non abbia acquisito i diritti (Dlg. 29 dicembre 1992 n. 518 - Tutela giuridica del software; Legge 18 agosto 2000, n. 248 - Nuove norme di tutela del diritto d'autore).

4.7 Non è consentito agli utenti modificare le caratteristiche impostate sui Personal Computer assegnati, i punti rete di accesso, le configurazioni delle reti e la configurazione del Browser per la navigazione, salvo autorizzazione esplicita dell'Amministratore di sistema.

4.8 E' responsabilità del dirigente verificare il coerente utilizzo delle risorse informatiche assegnate ed evitarne l'uso improprio o l'accesso da parte di personale non autorizzato, compreso l'utilizzo da parte di terzi di punti rete in luoghi non presidiati.

4.9 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 il Personal Computer 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. A tal fine è necessario attivare il blocco del Personal Computer ogni qual volta venga lasciato incustodito.

4.10 Non è consentito l'uso sul proprio Personal Computer di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, pc portatili, pendrive USB, telefoni cellulari, ed apparati in genere). Le informazioni e i dati potranno essere copiati o riprodotti in tutto o in parte solo per esigenze operative strettamente connesse allo svolgimento delle attività lavorativa.

4.11 E' fatto divieto di divulgare e comunicare in qualunque modo o forma le informazioni, i dati e le conoscenze riservati a soggetti che non siano autorizzati. Tali informazioni, dati e conoscenze dovranno essere utilizzati nella misura e con mezzi strettamente necessari allo svolgimento delle attività lavorativa.

4.12 E' vietato rimuovere, danneggiare deliberatamente o asportare componenti hardware.

Art. 5 - Gestione assegnazione delle credenziali di autenticazione

5.1 Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), assegnato dall'Amministratore di Sistema associato ad una parola chiave (password) riservata che dovrà venir custodita dall'incaricato con la massima diligenza e non divulgata. Non è consentita l'attivazione o la modifica della password di accensione (bios), senza preventiva autorizzazione da parte dell'Amministratore di Sistema.

5.2 Le password di ingresso alla rete, di accesso ai programmi sono previste ed attribuite dell'Amministratore di Sistema, previa formale richiesta del Responsabile dell'ufficio/area nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente.

5.3 La password, formata da lettere (maiuscole o minuscole) e/o numeri, anche in combinazione fra loro, deve essere composta da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato (per es. nomi/date di nascita e simili).

5.4 La password utilizzata dagli incaricati al trattamento, va modificata al primo utilizzo e, successivamente, almeno ogni tre o sei mesi, a seconda che i dati trattati siano rispettivamente sensibili e giudiziari oppure comuni.

5.5 La password deve essere immediatamente sostituita nel caso si sospetti che la stessa abbia perso la segretezza.

5.6 Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia all'Amministratore di Sistema.

5.7 E' dato incarico ai dirigenti di comunicare tempestivamente eventuali cambi di mansione che comportino modifiche o revoche di autorizzazione all'accesso delle risorse informatiche, sia all'ufficio del personale che all'Amministratore di Sistema, per iscritto, al fine di rendere possibili le modifiche dei profili di accesso alle risorse e la sostituzione delle password ove necessario.

Art. 6 - Utilizzo della rete comunale

6.1 Hanno diritto ad accedere alla rete comunale tutti i dipendenti, gli amministratori, le ditte fornitrici di software e/o servizi per motivi di manutenzione e limitatamente alle applicazioni di loro competenza (con apposita nomina a Responsabile del trattamento ai sensi dell'art. 29 del D.Lgs 196/2003), collaboratori esterni impegnati nelle attività istituzionali per il periodo di collaborazione.

6.2 Le cartelle utenti, che risiedono su server, 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 salvato, nemmeno per brevi periodi, in queste unità, sulle quali potranno essere svolte regolari attività di controllo, amministrazione e backup da parte dell'AdS.

6.3 L'utente è tenuto ad osservare le direttive dell'AdS volte a garantire il corretto funzionamento delle procedure di backup. I dati, documenti o file creati o modificati attraverso le applicazioni di produttività individuale (es. office o open-office) se salvati in cartelle utenti che risiedono su server sono soggetti alle procedure di backup da parte del personale del Sistema Informativo. Diversamente, per i dati salvati in locale (es. disco C: interno al Personal Computer) la responsabilità del backup, almeno settimanale, è a carico del singolo utente.

6.4 Le password di accesso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure definite. E' assolutamente proibito entrare nella rete e nei programmi con nomi utente diversi dal proprio.

6.5 L' Amministratore di Sistema può in qualunque momento procedere alla rimozione di file o applicazione che riterrà essere pericolosi per la sicurezza, siano essi presenti sui Personal Computer degli utenti che sulle unità di rete.

6.6 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. E' utile evitare un'archiviazione ridondante.

6.7 E’ vietato monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività degli utenti, leggere copiare o cancellare file e software di altri utenti, senza averne l'autorizzazione esplicita.

Art. 7 - Utilizzo dei supporti magnetici/ottici/ottici

7.1 Tutti i supporti magnetici/ottici/ottici rimovibili utilizzabili (floppy disk, cassette, cartucce, CD e DVD riscrivibili, supporti USB, etc.) contenenti dati sensibili devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.

7.2 Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici/ottici/ottici rimovibili contenenti dati sensibili, ciascun utente dovrà seguire le istruzioni dal personale del Sistema Informativo.

7.3 I supporti magnetici/ottici contenenti dati sensibili e/o giudiziari devono essere custoditi in armadi chiusi a chiave.

7.4 Non è consentito scaricare file contenuti in supporti magnetici/ottici/ottici non aventi alcuna attinenza con la propria prestazione lavorativa.

7.5 Tutti i file di provenienza incerta, ancorché potenzialmente attinenti all'attività lavorativa, non devono essere utilizzati/installati/testati. Nel caso di effettiva necessità di impiego devono essere sottoposti ad un preventivo controllo ed alla relativa autorizzazione all'utilizzo dell’AdS.

Art. 8 - Utilizzo di Personal Computer portatili

8.1 Ai Personal Computer portatili si applicano le regole di utilizzo previste per i Personal Computer connessi alla rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.

8.2 I Personal Computer portatili utilizzati all'esterno (convegni, riunioni, etc.), in caso di allontanamento, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.

8.3 Eventuali configurazioni di tipo Accesso Remoto, dirette verso la rete aziendale o attraverso internet, devono essere autorizzate esclusivamente a cura dell’Amministratore di Sistema.

Art. 9 - Uso della posta elettronica

9.1 La casella di posta elettronica (@comune.bracciano.rm.it) è uno strumento di lavoro e l’utente alla quale è assegnata è responsabile del corretto utilizzo della stessa. Si rammenta che i sistemi di posta elettronica non consentono al momento di garantire la riservatezza delle informazioni trasmesse: Si raccomandano gli utenti di non inoltrare dati ed informazioni classificabili "sensibili" o "riservate" con questo mezzo.

9.2 E' fatto divieto di utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mailing list non attinenti la propria attività o funzione svolta per l'ente, salvo diversa ed esplicita autorizzazione.

9.3 E' 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.

9.4 E' possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario, ma di norma per la comunicazione ufficiale a privati è obbligatorio avvalersi degli strumenti tradizionali di posta cartacea o di posta elettronica certificata.

9.5 E' obbligatorio controllare con il software antivirus i file allegati di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

9.6 Al fine di soddisfare le esigenze di un regolare svolgimento dell'attività lavorativa con quelle del rispetto della segretezza delle informazioni, in caso di assenza programmata degli utenti (ad es. per ferie o attività di lavoro fuori sede) è opportuno che l'AdS metta a disposizione degli stessi apposite funzionalità per l'invio automatico di messaggi di risposta contenenti le "coordinate" di posta elettronica di un altro soggetto o altre utili modalità di contatto. In tal caso, la funzionalità deve essere attivata dall'utente.

9.7 In caso di assenza non programmata (ad es. per malattia) la procedura - qualora non possa essere attivata dall'utente avvalendosi del servizio web mail -, potrebbe essere attivata a cura dell'ente, avvisando preventivamente l'utente stesso.

9.8 Sarà comunque consentito all'utente, in previsione di un'assenza prolungata, delegare un altro utente (fiduciario) ad accedere alla propria casella di posta elettronica per improrogabili necessità legate all'attività lavorativa. A cura del titolare del trattamento, di tale attività dovrebbe essere redatto apposito verbale e informato l'utente interessato alla prima occasione utile.

Art. 10 - Uso della rete internet e dei relativi servizi

10.1 Per ragioni di sicurezza e per garantire l'integrità dei sistemi informatici, l'accesso ad internet effettuato tramite elaboratori connessi alla rete comunale è scrupolosamente protetto da appositi dispositivi di sicurezza informatica (firewall, antivirus, proxy server, etc.).

10.2 Il Personal Computer abilitato alla navigazione in internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. E' proibita la navigazione in internet per motivi diversi da quelli funzionali all'attività lavorativa stessa.

10.3 E' fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti internet, nonché il download di file multimediali se non espressamente autorizzato dell'Amministratore di Sistema.

10.4 E' 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 o attinenti i compiti e le mansioni assegnate e con il rispetto delle normali procedure di acquisto.

10.5 E' 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), se non attinenti l'attività lavorativa svolta.

10.6 Non è consentita l'accesso a siti e a materiale dai contenuti di natura oltraggiosa e/o discriminatoria per sesso/etnia/religione/opinione e/o appartenenza sindacale e/o politica.

10.7 Al fine di evitare l'accesso a siti non pertinenti all'attività lavorativa, l'ente rende peraltro nota l'adozione di uno specifico sistema di blocco o filtro automatico che prevengano determinate operazioni quali l'upload o l'accesso a determinati siti inseriti in una black list.

Art. 11 - Accesso ai dati trattati dall'utente

11.1 Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.) o per finalità di controllo e programmazione dei costi aziendali (ad es. verifica costi di connessione ad internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, nel rispetto dell'art. 4, comma 2, della legge 300/1970 (Statuto dei Lavoratori), è facoltà dell'ente, tramite il personale del Sistema informativo o addetti alla manutenzione, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici aziendali e ai documenti ivi contenuti.

Art. 12 - Sistemi di controlli graduali

12.1 In caso di riscontrate anomalie, il personale incaricato del Sistema Informativo effettuerà controlli anonimi che si concluderanno con avvisi generalizzati diretti ai dipendenti dell'area o del settore in cui è stata rilevata l'anomalia, nei quali si evidenzierà l'utilizzo irregolare degli strumenti aziendali e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

12.2 Controlli su base individuale potranno essere computi solo in caso di successive ulteriori anomalie. Gli eventuali controlli potranno avvenire mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta. Il controllo sui file di log non è continuativo ed i file stessi vengono conservati solo per il tempo indispensabile, in conformità alla normativa vigente.

12.3 I sistemi software devono essere programmati e configurati in modo da cancellare periodicamente ed automaticamente (attraverso procedure di sovraregistrazione come, ad es. la cd. rotazione dei log file) i dati personali relativi agli accessi ad internet e al traffico telematico, la cui conservazione non sia necessaria.

12.4 In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

Art. 13 - Osservanza delle disposizioni in materia di Privacy

13.1 E' obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza. Tale norma andrà indicata nelle lettere di individuazione dell'incaricato al trattamento dei dati ai sensi dell'art. 30 del D.lgs 196/03.

Art. 14 - Sanzioni

14.1 Il mancato rispetto o la violazione delle regole contenute nel presente regolamento costituisce violazione degli obblighi e dei doveri del dipendente pubblico e, pertanto, in relazione alla gravità dell'infrazione, i dirigenti responsabili, previo espletamento di procedimento disciplinare, possono procedere all'applicazione delle sanzioni previste dalle disposizioni contrattuali vigenti in materia.

Art. 15 - Aggiornamento e revisione

15.1 I contenuti del presente regolamento andranno aggiornati nei casi di modifiche normative in materia di trattamento dei dati personali oppure quando ritenuto necessario dall'ente.

Art. 16 - Pubblicità

16.1 Il presente regolamento viene consegnato a ciascun utente del Comune di Bracciano, che firma per ricevuta. L'utente deve attenersi, nell'utilizzo e nella gestione delle risorse strumentali informatiche comunali, ai principi e ai doveri stabiliti nel "Codice di comportamento dei dipendenti delle pubbliche amministrazioni" D. M. 31 marzo 1994 - Ministero per la Funzione Pubblica.