Comune di Bientina

Provincia di Pisa

REGOLAMENTO PER IL CORRETTO UTILIZZO DELLE RISORSE INFORMATICHE E TELEMATICHE

Art. 1 – Oggetto

Il presente regolamento disciplina le condizioni per il corretto utilizzo degli strumenti informatici, l'uso della posta elettronica e la navigazione in internet ai sensi del codice dell'amministrazione digitale - D. Lgs. 82/2005, della Deliberazione del Garante per la protezione dei dati personali del 1 marzo 2007 "Linee guida per posta elettronica e internet" e della Direttiva del Dipartimento della Funzione Pubblica n. 02/09.

Il regolamento fornisce pertanto i parametri per disciplinare compiutamente e a norma di legge l'innovazione nella pubblica amministrazione.

Art. 2 - Modalità di utilizzo dei personal computer

2.1 - L'accesso all'elaboratore è protetto da password per la cui disciplina si rimanda all'articolo 3 del presente regolamento.

2.2 - La configurazione iniziale di ogni personal computer avvenuta ad opera di personale informatico addetto non deve essere modificata.

2.3 - Non è consentito installare autonomamente programmi di qualunque tipo, se non previa verifica, da parte del responsabile della gestione e manutenzione degli strumenti elettronici, di compatibilità con gli altri programmi software in uso. L'installazione sarà comunque effettuata dal personale informatico addetto su indicazione del responsabile della gestione e della manutenzione degli strumenti elettronici.

Ogni utente è personalmente responsabile del software installato sul pc a lui in dotazione; eventuali installazioni di software effettuate senza autorizzazione del responsabile della gestione e manutenzione degli strumenti elettronici sono di totale responsabilità dell'utente che ne risponderà personalmente in caso di violazione di licenza; in caso di dubbio sul software installato e sulle licenze di tale software è necessario informare per iscritto il responsabile della gestione e manutenzione degli strumenti elettronici il quale verificata o meno la presenza di regolare licenza deciderà se rimuovere il software dal personal computer.

2.4 - E' onere dei responsabili di ciascun servizio del Comune di Bientina, verificare il coerente utilizzo delle risorse assegnate ed evitarne l'uso improprio o l'accesso alle risorse da parte di personale non autorizzato, compreso l'utilizzo da parte di terzi di punti rete in luoghi non presidiati.

2.5 - Il personal computer deve essere spento ogni sera prima di lasciare gli uffici. In caso di assenze temporanee dall'ufficio, l'elaboratore, se non viene spento, deve essere lasciato disconnesso oppure deve essere attivato lo screensaver con password abilitata.

2.6 - Non è consentito collegare direttamente sul proprio pc o mediante rete LAN nessun dispositivo di memorizzazione, comunicazione o altro (masterizzatori, modem, pc portatili ed apparati in genere), se non

previa approvazione da parte del responsabile della gestione e manutenzione degli strumenti elettronici.

2.7 - Per quanto riguarda il trattamento dei dati sensibili, vengono individuati dei profili di autorizzazione per ciascun utente incaricato o per classi omogenee di utenti incaricati, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento. Periodicamente, e comunque almeno annualmente, verrà verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione, secondo quanto previsto ai punti 12, 13, 14 del disciplinare tecnico in materia di misure minime di sicurezza (allegato B al D. Lgs. 196/03) e dal documento programmatico sulla sicurezza aggiornato annualmente secondo quanto previsto dalla legge.

2.8 - Ogni utente relativamente ai supporti di memorizzazione dati di terze parti (CD, floppy, chiavi USB), deve rispettare quanto previsto dal successivo art. 10 del presente Regolamento relativo alle procedure di protezione antivirus.

2.9 - Non è consentita la compilazione, ricerca, diffusione e memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

Art. 3 - Utilizzo della rete del Comune di Bientina

3.1 - Le risorse di rete che trasferiscono i dati dell'ente devono essere esclusivamente impiegate da parte degli utenti e ciascuno ne è responsabile del corretto utilizzo; non ne è consentito l'uso da parte di persone non autorizzate. Dell'osservanza della presente norma risponde il responsabile di ciascun servizio.

3.2 - Le unità di memorizzazione di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Su queste unità, il responsabile della gestione e manutenzione degli strumenti elettronici deve svolgere regolari attività di controllo, amministrazione e backup.

3.3 - Le password d'ingresso alla rete ed ai programmi sono segrete e sono comunicate e gestite secondo le procedure previste all'art. 4.

3.4 - Il responsabile della gestione e manutenzione degli strumenti elettronici può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza sia sulle unità di rete sia sui pc degli incaricati (in quest'ultimo caso è necessario il preavviso da parte del responsabile agli eventuali interessati).

3.5 - Costituisce buona regola di gestione delle unità di memorizzazione di rete da parte degli utenti, la periodica (almeno ogni tre mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, al fine di agevolare le copie di sicurezza.

3.6 - Non è consentito collegare qualsiasi dispositivo alla rete aziendale senza la preventiva autorizzazione scritta del responsabile della gestione e manutenzione degli strumenti elettronici previa verifica della conformità agli standard tecnici presenti.

3.7 - Non è consentito all'utente modificare le caratteristiche impostate sui pc forniti, i punti rete di accesso e le configurazioni delle reti LAN/WAN presenti nelle sedi; eventuali modifiche strutturali dovranno essere concordate con il responsabile della gestione e manutenzione degli strumenti elettronici per garantire la compatibilità con la struttura preesistente.

Art. 4 - Gestione delle Password

4.1 - La gestione delle password è regolata dal Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del D. Lgs. 196/03) e da quanto previsto dal documento programmatico sulla sicurezza adottato dal Comune di Bientina.

4.2 - La password è strettamente personale e deve essere custodita dall'utente con la massima diligenza e non divulgata.

Le password di ingresso alla rete, di accesso ai programmi e dello screensaver, sono attribuite inizialmente dal responsabile della gestione e manutenzione degli strumenti elettronici e devono essere immediatamente sostituite dagli utenti.

4.3 - Le password devono essere lunghe almeno 8 caratteri, salvo impedimenti tecnici delle applicazioni, formate da lettere maiuscole e/o minuscole, numeri e caratteri speciali quali & % ^ # $, ricordando che lettere maiuscole e minuscole hanno significati diversi per i sistemi, evitando ovviamente contenuti di senso logico immediato che sono facilmente individuabili (per es. nomi/date di nascita e simili).

4.4 - Le password utilizzate dagli utenti hanno una durata massima di 6 mesi, che è pari altresì a 3 mesi per quegli utenti che trattano dati sensibili e/o giudiziari trascorsi i quali devono essere sostituite. Ogni nuova password deve essere fornita, in busta chiusa, all'incaricato della custodia delle credenziali.

4.5 - La password deve essere immediatamente sostituita, dandone comunicazione all'incaricato della custodia delle credenziali, nel caso si sospetti che la stessa abbia perso la segretezza.

4.6 - Qualora l'utente venga a conoscenza delle password di altro utente, è tenuto a comunicarglielo immediatamente ed in caso di impossibilità al suo Responsabile che lo comunicherà al responsabile della gestione e manutenzione degli strumenti elettronici affinché avvii la procedura per la sostituzione della password violata.

4.7 - E' dato incarico ai responsabili dei servizi di comunicare entro le successive 24 ore l'utilizzo delle risorse informatiche da parte degli utenti che a qualunque titolo debbano accedere alle stesse; con le stesse modalità dovranno essere comunicati eventuali cambi di mansione che comportino modifiche o revoche di autorizzazione all'accesso delle risorse informatiche al responsabile della gestione e manutenzione degli strumenti elettronici.

4.8 - Il presente articolo costituisce diretta applicazione del punto 5–6 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al D. Lgs. 196/03) cui si rinvia per quanto non espressamente previsto.

Art. 5 - Utilizzo dei supporti di memorizzazione removibili

5.1 - I dati sensibili o giudiziari, contenuti in supporti di memorizzazione removibili riutilizzabili (cassette, cartucce, floppy, supporti dati e USB etc.), se non utilizzati, devono essere distrutti o resi inutilizzabili. Detti supporti possono essere riutilizzati da altri incaricati, non autorizzati al trattamento dei dati precedentemente memorizzati, se queste informazioni non sono intelligibili e tecnicamente in alcun modo ricostruibili.

5.2 - I supporti removibili contenenti dati sensibili e giudiziari sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendano temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettano di identificare gli interessati solo in caso di necessità.

5.3 - Non è consentito leggere files contenuti in supporti magnetici/ottici non aventi alcuna attinenza con la propria prestazione lavorativa.

5.4 - Tutti i files 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 da parte del responsabile della gestione e manutenzione degli strumenti elettronici.

Art. 6 - Utilizzo Stampanti

6.1 - 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 molto lunghi o di contenuto grafico su stampanti comuni.

6.2 - Non è consentito stampare documenti personali su qualsivoglia stampante, salvo giustificabili eccezioni, di cui comunque risponde personalmente l'utente.

Art. 7 - Utilizzo di pc portatili e/o accessori temporaneamente assegnati

7.1 - L'utente è responsabile del pc portatile e/o accessori (macchina fotografica, videoproiettore, telo…) temporaneamente assegnati dall'amministrazione e deve custodirli con diligenza sia durante gli spostamenti sia durante l'utilizzo, fino alla loro riconsegna.

7.2 - 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 sugli stessi prima della riconsegna.

7.3 - I pc portatili utilizzati all'esterno (convegni etc.), contenenti dati dell'ente, devono essere custoditi in un luogo protetto.

7.4 - Eventuali configurazioni di tipo Accesso Remoto, mediante linea telefonica sono a cura del responsabile della gestione e manutenzione degli strumenti elettronici. E' vietato utilizzare le suddette connessioni all'interno delle sedi comunali se contemporaneamente connessi alla rete LAN per la potenziale pericolosità di una doppia apertura verso l'esterno.

7.5 - I beni strumentali temporaneamente assegnati devono essere riconsegnati nei tempi stabiliti dall'assegnatario.

Art. 8 - Uso della posta elettronica

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

8.2 - E' fatto divieto di utilizzare le caselle di posta elettronica ……@comune.bientina.pi.it per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mailing-lists non attinenti la propria attività o funzione svolta per l'ente, salvo diversa ed esplicita autorizzazione, e salvo giustificabili eccezioni, di cui comunque rispondono personalmente le persone assegnatarie delle caselle di posta elettronica.

8.3 - La posta elettronica deve essere scaricata quotidianamente; in caso di assenza prolungata se ne deve dare comunicazione al responsabile della gestione e manutenzione degli strumenti elettronici.

8.4 - Per la trasmissione di file all'interno del Comune di Bientina è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati: se di dimensioni superiori a 2 Mb alla capacità della casella di posta, si possono utilizzare le directory di scambio (cartelle condivise allo scopo create su ogni pc)

presenti sui file server, notificando a mezzo mail al destinatario la disponibilità del file stesso.

8.5 - E' obbligatorio controllare con il software antivirus i file allegati di posta elettronica prima del loro utilizzo.

8.6 - E' vietato inviare catene telematiche (o di Sant'Antonio).

8.7 - Le informazioni riservate o relative a dati sensibili, se devono essere trasmesse, devono essere opportunamente protette con tecniche di cifratura a chiave asimmetrica.

8.8 - La casella di posta elettronica ……@comune.bientina.pi.it pur essendo talvolta nominativa non è personale, ma funzionale all'attività assegnata; è pertanto suscettibile, da parte del titolare del trattamento, dei necessari controlli su eventuali utilizzi, consapevolmente impropri del servizio, ricorrendo, ove necessario, alle autorità competenti.

Art. 9 - Uso della rete Internet e dei relativi servizi

9.1 - Il pc 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.

9.2 - E' fatto divieto scaricare software di qualunque tipo prelevato da siti Internet, se non espressamente autorizzato dal Responsabile della gestione e manutenzione degli strumenti elettronici.

9.3 - 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 di diretta autorizzazione o attinenti i compiti e le mansioni assegnate e con il rispetto delle normali procedure di acquisto.

9.4 - E' vietata la partecipazione a forum non professionali, l'utilizzo di chat lines (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.

9.5 - Il responsabile della gestione e manutenzione degli strumenti elettronici si riserva di applicare per singoli e gruppi di utenti, politiche di navigazione personalizzate in base alle mansioni, al fine di ottimizzare l'uso delle risorse, gli investimenti e le prestazioni delle connessioni esistenti. Tuttavia la responsabilità delle operazioni compiute durante la navigazione rimane a totale carico dell'utilizzatore.

9.6 - Non è consentito inoltre la ricerca di documenti informatici e la navigazione nei siti con contenuti di natura oltraggiosa e/o discriminatoria per sesso/etnia/religione/opinione e/o appartenenza sindacale e/o politica o comunque non attinenti all'attività lavorativa.

9.7 - La navigazione in internet può formare oggetto di controllo, seppur graduale, rispettando i principi di pertinenza e non eccedenza tenendo conto delle linee guida del Garante per posta elettronica e internet. Il sistema informatico dispone dei log della navigazione dei singoli utenti utilizzabili nel rispetto di quanto previsto dalla normativa sulla privacy.

Art. 10 - Protezione antivirus

10.1 - Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico mediante virus o mediante ogni altro software aggressivo.

10.2 - Il responsabile della gestione e manutenzione degli strumenti elettronici è tenuto a controllare il regolare funzionamento e l'aggiornamento periodico del software antivirus installato, secondo le procedure

previste.

10.3 - Nel caso che il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente: sospendere ogni elaborazione in corso senza spegnere il computer e segnalare l'accaduto al responsabile della gestione e manutenzione degli strumenti elettronici.

10.4 - Non è consentito l'utilizzo di pc, floppy disk, cd/dvd, dvd riscrivibili, chiavi USB di dubbia provenienza; in caso di necessità chiedere la validazione dal responsabile della gestione e manutenzione degli strumenti elettronici.

10.5 - Ogni dispositivo magnetico di provenienza esterna all'ente dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere consegnato al responsabile della gestione e manutenzione degli strumenti elettronici.

Art. 11 - Osservanza delle disposizioni in materia di Privacy

E' obbligatorio attenersi alle disposizioni in materia di Privacy in osservanza del D. Lgs. 196/03 e del disciplinare tecnico in materia di misure minime di sicurezza.

Art. 12 - Sanzioni

Il mancato rispetto o la violazione delle regole contenute nel presente Regolamento è perseguibile con le azioni civili e penali previste dalla normativa vigente in materia.

Art. 13 - Individuazione di ruoli

All'approvazione del presente regolamento, per l'individuazione dei vari ruoli si tenga conto di quanto previsto dal documento programmatico sulla sicurezza adottato dallo stesso Ente.