Regolamento per il corretto utilizzo

degli strumenti informatici e telematici

APPROVATO CON DELIBERAZIONE DEL CONSIGLIO COMUNALE N. __ DEL _____

Art. 1 Validità

Il presente regolamento è valido per tutta la rete dati del Comune di Bordighera, ivi compresi i PC, i Thin Client ed i server.
Deve essere utilizzata anche per i processi in cui è necessario l'ausilio di dotazioni informatiche ovvero con l'utilizzo di software e in tutte le attività di manutenzione hardware e software.

Art. 2 Utilizzo del Personal Computer e delle periferiche connesse

1. Il Personal Computer affidato al dipendente è uno strumento di lavoro. Ogni utilizzo non attinente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Tutti gli strumenti citati sono di esclusiva proprietà dell'Ente, messi a disposizione del lavoratore al solo fine dello svolgimento delle proprie mansioni lavorative.
2. L'accesso all'elaboratore deve essere protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata. La stessa password è attivata per l'accesso alla rete.
3. Non è consentito installare autonomamente software, poiché sussiste il grave pericolo di propagare virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore. Tali programmi verranno cancellati ed ogni violazione verrà automaticamente segnalata al dirigente competente.
4. Non è consentito l'uso di programmi diversi da quelli distribuiti ufficialmente dal Comune di Bordighera (D. Lgs. 518/92 sulla tutela giuridica del software e L. 248/2000 e successive modifiche ed integrazioni recante nuove norme di tutela del diritto d'autore).
5. Non è consentita l'installazione sul personal computer in dotazione di alcun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, …) ad eccezione di quelli in dotazione o di quelli installati per ragioni d'ufficio.
6. Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente l'ufficio informatica nel caso in cui siano rilevati virus informatici.
7. 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.
8. Non è possibile spostare personal computer, stampanti ed ogni altro apparato informatico collegato direttamente o indirettamente alla rete, se non in accordo con l'ufficio manutenzione e con l'ufficio informatica.
9. Il Personal Computer, il monitor, le stampanti locali e di rete devono essere spente al termine dell'attività lavorativa 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 provare in seguito l'indebito uso. In tali frangenti ogni responsabilità sarà addebitata al proprietario delle credenziali.

Art. 3 Utilizzo di dispositivi esterni di memorizzazione dati: chiavette usb, hard disk esterni, macchine fotografiche digitali, iPOD, lettori MP3, ecc.

1. E' vietato l'uso dei dispositivi esterni di memorizzazione su tutti i personal computer della rete, salvo diversa autorizzazione del Dirigente in accordo con il Responsabile dell'ufficio informatica, anche da parte di utenti generici, stagisti, consulenti ed in particolar modo su postazioni di front-office con servizi rivolti ai cittadini o ritenuti strategici al funzionamento dell'Ente.
2. E' vietato l'uso di dispositivi personali esterni all'Ente.
3. Il dispositivo di proprietà dell'Ente che risulta infetto da virus deve essere obbligatoriamente e tempestivamente consegnato direttamente dall'utente al Responsabile dell'ufficio informatica.
4. I supporti magnetici e digitali riutilizzabili (dischetti, cassette, chiavi USB …) contenenti dati personali 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. I supporti magnetici contenenti dati personali devono essere custoditi in archivi chiusi.
5. Non è consentito scaricare file contenuti in supporti magnetici/ottici (Hard Disk) non aventi alcuna attinenza con la propria prestazione lavorativa.
6. Eventuali danni derivanti dalla mancata osservanza del rispetto delle presenti norme saranno imputati al dipendente.

Art. 4 Particolari dispositivi esterni

1. E' vietato l'uso e/o l'installazione di software di collegamento/condivisione dati con i personal computer o portatili dei dispositivi, quali telefoni cellulari, navigatori satellitari, ecc, se non espressamente autorizzato dal responsabile del servizio e dall'ufficio informatica.
2. E' altresì vietato il collegamento alla rete dati comunale di dispositivi con connessioni di tipo Wireless, Bluetooth o di altra tipologia per scambio dati se non preventivamente autorizzati dal responsabile dell'ufficio e dall'ufficio informatica.
3. Per giustificati motivi, sentito il dirigente competente, è possibile attivare il collegamento al server per il lavoro da remoto (VPN). Il collegamento viene configurato dall'ufficio informatica con rilascio di apposite credenziali. Sul PC del dipendente deve essere attivato un adeguato sistema di controllo antivirus ed antispyware.

Art. 5 Utilizzo dei personal computer portatili

1. L'utente è responsabile dell'eventuale portatile assegnatogli che deve essere custodito con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
2. Ai portatili si applicano le regole di utilizzo previste per i personal computer connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.
3. E' vietato collegare in rete personal computer portatili non di proprietà dell'Ente (ad esempio consulenti, stagisti, pc personali, ecc), salvo diversa ed esplicita autorizzazione scritta del responsabile dell'ufficio e dall'ufficio informatica.
4. E' vietato collegare nel dominio comunale personal computer portatili. Non sarà dunque possibile configurare sul portatile utenze personali (ad esempio: nome.cognome), per accedere alla rete comunale, alle stampanti di rete, alle cartelle condivise ed ai programmi comunali.

Art. 6 Protezione antivirus

1. Il sistema di protezione contro virus informatici è monitorato dalla rete informatica comunale e l'aggiornamento dell'antivirus sui PC connessi in rete avviene in modo automatico.
2. Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico mediante virus o mediante ogni altro software aggressivo.
3. Si raccomanda di porre particolare attenzione all'utilizzo di floppy disk, cd rom, chiavette USB e memorie di massa.

Art. 7 Uso della posta elettronica comunale

1. La casella di posta, assegnata all'utente, è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse. E' fatto divieto di utilizzare le caselle di posta elettronica @bordighera.it per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o "mailing-list" non attinenti alla propria attività lavorativa, salvo diversa ed esplicita autorizzazione.
2. E' vietato partecipare a catene telematiche (o di Sant'Antonio).
3. E' buona norma evitare messaggi completamente estranei al rapporto di lavoro. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

5. Gli allegati alle mail in ingresso ed in uscita non possono superare la dimensione di 20 MB (per gli allegati di grandi dimensioni è disponibile un apposito spazio FTP).
7. E' vietato l'uso di programmi e/o servizi (esterni) di posta elettronica anonima che permettono di impersonare terze persone nei messaggi inviati.
8. Le password di ingresso al sistema di mail mediante Web sono previste ed attribuite inizialmente dall'Amministratore del sito internet comunale, vanno successivamente modificate e comunicate al custode delle credenziali.
9. E' vietato configurare account di posta elettronica diversi da quelli comunali sul proprio personal computer.

Art. 8 Navigazione Internet e relativi servizi

1. Il personal computer abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. Non è permessa la navigazione in Internet e ogni forma di registrazione a siti per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.
2. E' fatto divieto all'utente di scaricare e/o installare software e programmi, così pure scaricare musica, film, filmati e ogni altro file coperto da diritti d'autore.
3. E' vietata la partecipazione a Forum, l'utilizzo di chat, di bacheche elettroniche e le registrazioni in guest book, anche utilizzando pseudonimi (o nicknames) che non siano legati al lavoro e/o alla formazione professionale. E' vietata la partecipazione a social-network di qualunque natura (facebook, myspace, ..) nonché attività di "dating online". E' fatta salva specifica autorizzazione, da rilasciarsi da parte del dirigente competente, per collegamenti legati all'attività lavorativa e/o alla formazione professionale.

Art. 9 Controllo sull'utilizzo di internet e posta elettronica

1. Si rimanda all'Appendice al presente regolamento per quanto attiene alle modalità con le quali l'Ente potrà accertare e quindi reprimere le condotte illecite dei dipendenti utilizzatori di internet e della posta elettronica.

Art. 10 Utilizzo delle cartelle di rete

1. Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Su queste unità sono svolte regolari attività di controllo, amministrazione e backup da parte dell'ufficio informatica.
2. E' fatto particolare divieto di salvare file (anche compressi) di formato:
- Eseguibili (exe, cmd, reg, vbs)
- giochi, screen saver e comunque ogni file non attinenti all'attività lavorativa
- immagini in formato BMP (tali immagini devono essere convertite in formato JPG, JPEG al fine di occupare il minor spazio possibile).
3. Ad ogni utente è attribuita su File Server una cartella documenti a cui ha accesso esclusivo oltre a cartelle di ufficio a cui possono accedere gli utenti del medesimo settore e/o servizio per la condivisione dei file. Il Responsabile della Struttura può accedere a tutte le cartelle del proprio settore.
4. Per motivi di sicurezza è vietato condividere in altro modo cartelle fra utenti sul proprio PC, poiché possono costituire delle minacce ai dati custoditi, oltre a non ottemperare alle disposizioni di cui al D. Lgs. n. 196/2003.
5. L'Amministratore del Sistema può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza della rete dati sia sui PC degli incaricati sia sulle unità di rete.
6. Costituisce buona regola la periodica pulizia degli archivi (almeno ogni sei mesi), con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. E', infatti, assolutamente da evitare un'archiviazione ridondante.

7. Non è consentita la modifica dei permessi di accesso delle cartelle di rete da parte degli utenti.

Art. 11 Gestione delle Password

1. Le password d'ingresso alla rete ed ai programmi sono personali, segrete e vanno comunicate e gestite secondo le procedure di seguito delineate. E' assolutamente proibito entrare nella rete e nei programmi con altri nomi utente.
2. Le password di ingresso alla rete e di accesso ai programmi, sono previste ed attribuite inizialmente dall'Amministratore del Sistema. Successivamente deve essere effettuata l'autonoma sostituzione delle stesse da parte degli incaricati al trattamento. Almeno una volta all'anno le credenziali e password di accesso ai siti internet ai quali si è registrati per motivi di lavoro vanno comunicate all'ufficio personale in busta chiusa (Custode delle Copie delle Credenziali), mediante l'apposito modulo presente nello spazio condiviso, per la custodia delle credenziali.
4. La password deve avere le seguenti caratteristiche:
   - non deve contenere nomi comuni;
   - non deve contenere nomi di persona;
   - deve contenere sia lettere che numeri;
   - deve essere lunga almeno 9 caratteri;
   - non deve essere riconducibile all'incaricato
5. La password deve essere immediatamente sostituita, dandone comunicazione al Custode delle Copie delle Credenziali, nel caso si sospetti che la stessa abbia perso la segretezza.
6. In caso di smarrimento della password di accesso, l'utente deve comunicarlo all'Amministratore del Sistema che procederà a fornire una password provvisoria. L'utente, una volta connesso in rete, dovrà sostituirla e dovrà comunicarla al Custode delle Copie delle Credenziali.
7. In casi eccezionali l'Amministratore del Sistema è autorizzato alla sostituzione della password su richiesta dell'interessato.

Art. 12 Salvataggio dei dati (Backup)

1. L'utente è responsabile dei dati sul proprio PC; si è invitati a non salvare dati inerenti lì'attività lavorativa sul proprio PC ma sul Server, al fine di evitarne la perdita (es. nel caso in cui si guasti l'Hard Disk).
2. L'ufficio informatica esegue sistematicamente il salvataggio dei dati contenuti sui server secondo una policy definita.

Art. 13 Aggiornamenti

1. Gli aggiornamenti del sistema operativo sono necessari, oltre che essere un obbligo di legge, al fine di proteggere il PC e l'intera rete. Quando viene segnalata sul PC la disponibilità di nuovi aggiornamenti per il sistema è compito dell'utente provvedere al loro scaricamento ed installazione.

Art. 14 Installazione degli applicativi sui personal computer o su Server

1. Ogni intervento che richieda l'installazione o l'aggiornamento di software su personal computer o Server e comunque su apparati dell'Ente deve essere concordato con l'Amministratore del Sistema.
2. Tutte le installazioni dovranno essere assistite dal personale tecnico dell'Ente.
3. E' dato obbligo ai singoli utenti di trasmettere all'ufficio informatica i CD di installazione e l'eventuale documentazione forniti dalle Società o Enti esterni.

Art. 15 Gestione degli accessi alla rete e dei permessi

1. Tutte le richieste per eventuali abilitazioni, creazioni di utente, modifiche, ecc., dovranno essere comunicate all'ufficio informatica per il rilascio delle credenziali.

Art. 16 Richieste di assistenza tecnica (Help Desk)

1. L'attivazione di una chiamata per le richieste di assistenza tecnica hardware e/o software può avvenire mediante telefono oppure Internet rivolgendosi all'ufficio informatica.

Art. 17 Osservanza delle disposizioni in materia di Privacy

1. E' obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, così come comunicate con lettera di incarico per il trattamento dei dati dal dirigente del settore di competenza.
2. Il mancato rispetto o la violazione delle regole contenute nel D.Lgs. n. 196 del 30 giugno 2003 è perseguibile con le azioni civili e penali previste.
3. Il mancato rispetto delle norme contenute nel presente regolamento può comportare l'applicazione di sanzioni disciplinari, in ottemperanza alle disposizioni disciplinari di cui ai CCNL e del D.Lgs. 150/2009.
4. Il presente regolamento, unitamente all'allegato sul controllo a distanza dei lavoratori relativamente all'utilizzo di internet e della posta elettronica, integra il codice disciplinare dell'Ente, ai sensi dell'art. 54 – comma 5 – del D. Lgs. n. 165/2001 ed è soggetto ad affissione all'Albo Pretorio dell'Ente e in luogo accessibile a tutti i dipendenti, e a pubblicazione sul sito internet comunale.

Art. 18 Entrata in vigore

Il presente regolamento e la sua appendice allegata entrano in vigore 25 giorni dopo la pubblicazione all'albo pretorio on-line della delibera di approvazione e copia del regolamento e dell'appendice sono pubblicate in via permanente sul sito internet comunale.

Appendice al "Regolamento per il corretto utilizzo degli strumenti informatici e telematici" sul controllo a distanza dei lavoratori relativamente all'utilizzo di internet e posta elettronica

Articolo 1a – Oggetto

La presente disciplina regola le modalità con le quali il Comune di Bordighera potrà accertare e quindi reprimere le condotte illecite dei dipendenti utilizzatori di internet e della posta elettronica, ai sensi dell'art. 4 della legge 300/70 (Statuto dei Lavoratori).

Articolo 2a – Controllo sull'utilizzo di Internet: siti web interdetti

Il Comune di Bordighera filtra l'accesso ai contenuti della rete Internet tramite un software automatico di filtraggio. Eventuali deroghe all'accessibilità dei siti interdetti dovranno essere autorizzate dal dirigente responsabile e richieste all'ufficio informatica, qualora tale accessibilità sia funzionale alle esigenze di servizio.

Articolo 3a – Modalità e limiti dei controlli sull'utilizzo di internet

Ai soli fini di accertare e quindi reprimere condotte illecite dei lavoratori utilizzatori di internet l'Ente può, a sua tutela, effettuare verifiche a campione o anche in via sistematica sugli accessi effettuati mediante idonei programmi diagnostici informatici. E' comunque esclusa la possibilità di effettuare controlli sugli accessi internet mediante impianti audiovisivi.

Art. 4a – Repressione dell'abuso di internet

Qualora, ad esito del controllo, l'Ente rilevi delle anomalie sull'utilizzo di internet che possano essere configurate quali abusi, si procederà a comunicare l'avvio del procedimento disciplinare all'interessato e, per conoscenza, al relativo Responsabile della Struttura. A seguito dell'accertamento della condotta illecita e, quindi, dell'adozione del provvedimento disciplinare l'Ente procederà altresì a segnalare all'Autorità competente o a reprimere l'abuso secondo la normativa vigente.
Ai fini della corretta interpretazione della presente disciplina, per abuso di utilizzo di internet, oltre all'uso in difformità di quanto disciplinato dal "Regolamento per il corretto utilizzo degli strumenti informatici e telematici", si intende quanto segue:
- visita di siti web per motivi non pertinenti al proprio servizio o alla propria funzione, attuata con modalità e tempi tali da incidere negativamente sull'ordinaria attività;
- visita di siti web interdetti;
- scaricare e installare software senza una preventiva autorizzazione del Responsabile della Struttura;
- manomissioni dei sistemi di protezione e/o delle configurazioni dei personal computer;
- azioni aventi rilevanza penale, con riferimento a qualunque condotta penalmente rilevante anche se non contemplata fra i reati contro la Pubblica Amministrazione;
- azioni commesse con dolo o colpa grave che mettano a repentaglio la sicurezza e l'integrità del sistema informatico comunale e dei dati personali trattati;
- azioni in frode alle misure di sicurezza comunque inerenti i punti precedenti.

Art. 5a – Utilizzo di posta elettronica - Tutela preventiva

Il Comune di Bordighera dà attuazione a quanto previsto dalla Deliberazione n. 13/2007 del Garante per la protezione dei dati personali e, pertanto:
- il datore di lavoro rende disponibili, laddove possibile, indirizzi di posta elettronica istituzionali condivisi tra più lavoratori;

- in previsione della possibilità che, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica, l'interessato deve essere messo in grado di delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Il fiduciario deve essere designato dal dipendente.

Art. 6a – Controllo a distanza sull'utilizzo della posta elettronica

Così come altresì precisato dall'art. 7 del vigente "Regolamento per il corretto utilizzo degli strumenti informatici e telematici", le caselle di posta elettronica istituzionale sono strumenti di lavoro.
Ai soli fini di accertare e quindi reprimere condotte illecite dei lavoratori utilizzatori della posta elettronica l'Ente può, a sua tutela, effettuare verifiche a campione od anche in via sistematica mediante idonei programmi diagnostici informatici. E' comunque esclusa la possibilità di effettuare controlli sull'utilizzo della posta elettronica mediante impianti audiovisivi.
Le presenti disposizioni inerenti il controllo a distanza dell'utilizzo di internet sono estese, in quanto applicabili, al controllo previsto dal presente articolo sull'utilizzo della posta elettronica, con le precisazioni di seguito riportate.
In via generale il controllo difensivo dell'Ente potrà essere eventualmente esercitato in relazione ai destinatari delle e-mail in uscita.
Relativamente alle e-mail in entrata, il controllo difensivo dell'Ente potrà essere esercitato sui mittenti solamente per verificare l'eventuale avvenuta iscrizione degli utilizzatori della posta elettronica a mailing list per motivi non istituzionali o non pertinenti al servizio o alle funzioni svolte, con conseguente abuso dell'utilizzo di internet che non sia stato precedentemente rilevato.
Per abuso di utilizzo della posta elettronica si intende quanto segue:
- nel caso di iscrizione a mailing list, visita di siti web per motivi non pertinenti al proprio servizio o alla propria funzione, attuata con modalità e tempi tali da incidere negativamente sull'ordinaria attività di servizio, qualora ciò non abbia rilevanza penale;
- nel caso di iscrizione a mailing list, visita a siti web interdetti;
- farsi inviare software;
- diffusione di software di proprietà dell'ente o di terzi,
- diffusione di banche dati di cui l'Ente sia titolare;
- utilizzo di funzionalità informatiche già rese disponibili dall'Ente;
- utilizzo della posta elettronica per scopi puramente privati;
- azioni aventi rilevanza penale, con riferimento a qualunque condotta penalmente rilevante anche se non contemplata fra i reati contro la Pubblica Amministrazione;
- azioni in frode alle misure di sicurezza inerenti i punti precedenti.
E' esclusa qualsiasi forma di controllo sull'utilizzo della posta elettronica diversa da quelle previste nel presente articolo.

Art. 7a – Pubblicità

Il dirigente dell'ufficio personale è incaricato di rendere noto il contenuto della presente disciplina ai dipendenti del Comune di Bordighera mediante affissione del medesimo all'Albo Pretorio dell'Ente e in luogo accessibile a tutti i dipendenti, e mediante pubblicazione sul sito internet comunale, nonché alle organizzazioni sindacali a mezzo informativa successiva.