



Allegato alla Delib. G.M. n.200 del 24/09/2009

**Regolamento interno per l'utilizzo del Sistema
Informatico
del Comune di Ceglie Messapica**



(Il presente regolamento è stato redatto tenendo conto delle linee guida del Garante della Privacy)

Indice

Premessa

1. Campo di applicazione
2. Utilizzo del Personal Computer
3. Gestione ed assegnazione delle credenziali di autenticazione
4. Utilizzo della rete
5. Utilizzo e conservazione dei supporti rimovibili
6. Utilizzo di PC portatili
7. Uso della posta elettronica
8. Navigazione in Internet
9. Protezione antivirus
10. Utilizzo dei telefoni, fax e fotocopiatrici aziendali
11. Osservanza delle disposizioni in materia di Privacy
12. Accesso ai dati trattati dall'utente
13. Sistema di controlli graduali
14. Sanzioni
15. Aggiornamento e revisione
16. Entrata in vigore del regolamento e pubblicità



Premessa

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete Internet dai Personal Computer, espone *la Rete del Comune di Ceglie Messapica e dipendenti* a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (legge sul diritto d'autore e legge sulla privacy, fra tutte), creando evidenti problemi alla sicurezza ed all'immagine dello stesso Comune.

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro, **il Comune di Ceglie Messapica ha adottato un Regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati.**

Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni già fornite a tutti gli incaricati in attuazione del D.Lgs. 30 giugno 2003 n. 196 e del Disciplinare tecnico (Allegato B al citato decreto legislativo) contenente le misure minime di sicurezza, nonché integrano le informazioni già fornite agli interessati in ordine alle ragioni e alle modalità dei possibili controlli o alle conseguenze di tipo disciplinare in caso di violazione delle stesse.

1. Campo di applicazione

- 1.1 Il nuovo regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori del Comune a prescindere dal rapporto contrattuale con lo stesso intrattenuto (lavoratori somministrati, collaboratori a progetto, in stage, ecc.) ed a chiunque per dovesse utilizzare le risorse informatiche del Comune di Ceglie Messapica.
- 1.2 Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni utilizzatore a cui vengono concesse specifiche credenziali di autenticazione. Tale figura potrà anche venir indicata quale "incaricato del trattamento".

2. Utilizzo del Personal Computer

- 2.1 **Il Personal Computer affidato all'utente è uno strumento di lavoro.** Ogni utilizzo non inerente all'attività lavorativa o istituzionale è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Il Personal Computer deve essere custodito con cura evitando ogni possibile forma di danneggiamento.
- 2.2 Il Personal Computer dato in affidamento all'utente permette l'accesso alla rete del Comune di Ceglie Messapica solo attraverso specifiche **credenziali di autenticazione** come meglio descritto al successivo punto 3 del presente Regolamento.
- 2.3 Il Comune di Ceglie Messapica rende noto che il personale incaricato che opera presso il Servizio Informatico Comunale (nel seguito per brevità "Servizio I.C.") è stato autorizzato a 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.). Detti interventi, in considerazione dei divieti di cui ai successivi punti n° 7.3 e 8.1, 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 del Comune, si applica anche in caso di assenza prolungata od impedimento dell'utente.

- 2.4 Il personale incaricato del servizio S.I.C. ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC 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 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, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.
- 2.5 Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal personale del Servizio S.I.C. per conto del Comune, né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione espone lo stesso Ente a gravi responsabilità civili; si evidenzia inoltre che le violazioni della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate anche penalmente.
- 2.6 Salvo preventiva espressa autorizzazione del personale del Servizio S.I.C., non è consentito all'utente modificare le caratteristiche impostate sul proprio PC né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ...).
- 2.7 Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale del Servizio S.I.C. nel caso in cui siano rilevati virus ed adottando quanto previsto dal successivo punto n° 9 del presente Regolamento relativo alle procedure di protezione antivirus.
- 2.8 Il Personal Computer deve essere spento prima di lasciare gli uffici per fine giornata di lavoro o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo. 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.

3. Gestione ed assegnazione delle credenziali di autenticazione

- 3.1 Le credenziali di autenticazione per l'accesso alla Rete Comunale vengono inizialmente assegnate dal personale del Servizio S.I.C. e successivamente resettate dal dipendente stesso secondo criteri prestabiliti.
- 3.2 Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), assegnato dal Servizio S.I.C., associato ad una parola chiave (password) riservata e creata dall'incaricato che dovrà essere **memorizzata, custodita con la massima diligenza, non divulgata**. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte del Servizio S.I.C.



- 3.3 La parola chiave deve essere formata da 8 o più caratteri appartenenti ad almeno tre delle seguenti quattro categorie: lettere maiuscole, lettere minuscole, numeri, caratteri speciali¹, anche in combinazione fra loro e non deve contenere riferimenti agevolmente riconducibili all'incaricato.
- 3.4 La password di accesso di ciascun incaricato sarà automaticamente resettata ogni tre mesi. In base a tale procedura automatica, l'incaricato, mediante avviso a video, dovrà inserire ogni 3 mesi una password nuova, diversa dalla precedente.
- 3.5 L'utente potrà richiedere la modifica della parola chiave al personale del Servizio S.I.C., per decorrenza del termine sopra previsto e/o in caso di perdita della riservatezza.
- 3.6 Soggetto preposto alla custodia delle credenziali di autenticazione è il personale incaricato del Servizio S.I.C. del Comune di Ceglie Messapica.

4. Utilizzo della Rete

- 4.1 Per l'accesso alla rete del Comune di Ceglie Messapica ciascun utente deve essere in possesso delle specifiche credenziali di autenticazione.
- 4.2 È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente di un altro operatore. Le parole chiave d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.
- 4.3 **Le cartelle utenti presenti nel server storage sono aree di condivisione** di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. **I documenti di lavoro dovranno essere tutti memorizzati nella cartella My Documents (Documenti) del Desktop Utente. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in questa cartella.** Su queste unità vengono svolte regolari attività di controllo, amministrazione e back up da parte del personale del Servizio S.I.C.
Si ricorda che tutti i dischi o altre unità di memorizzazione locali (es. disco C: del proprio PC) non sono soggette a salvataggio da parte del personale incaricato del Servizio S.I.C. La responsabilità del salvataggio dei dati eventualmente ivi contenuti è pertanto a carico del singolo utente.
- 4.4 Il personale del Servizio S.I.C. 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.
- 4.5 Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante. E' fatto divieto salvare files musicali, video e similari sul Pc in dotazione dell' Ente. **Ogni dipendente del Comune avrà una soglia massima di spazio disco di circa 200 Mb, pertanto in caso di superamento della soglia limite per validi e giustificati motivi, sarà necessario contattare il Responsabile del Servizio S.I.C.**

¹ Per caratteri speciali si intendono tutti i caratteri della tastiera non definiti come lettere o numeri.



5. Utilizzo e conservazione dei supporti rimovibili

- 5.1 Al fine di evitare che documenti o atti amministrativi contenenti dati sensibili possano essere trafugati o alterati, saranno abilitati all'utilizzo di supporti magnetici rimovibili (CD e DVD riscrivibili, supporti USB, ecc.) solo quelle postazioni preventivamente autorizzate dai responsabili di area.
In tal caso gli utenti abilitati dovranno usare particolare cautela nell'utilizzo di tali supporti specie se contenenti dati sensibili o informazioni costituenti know-how aziendale, onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.
- 5.2 Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, ciascun utente dovrà contattare il personale del Servizio S.I. e seguire le istruzioni da questo impartite.
- 5.3 In ogni caso, i supporti magnetici contenenti dati sensibili devono essere dagli utenti adeguatamente custoditi in armadi chiusi.
- 5.4 E' vietato l'utilizzo di supporti rimovibili personali.
- 5.5 L'utente è responsabile della custodia dei supporti e dei dati comunali in essi contenuti.

6. Utilizzo di PC portatili

- 6.1 L'utente è responsabile del PC portatile assegnatogli dal Servizio S.I. e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nei luoghi di lavoro.
- 6.2 Ai PC portatili si applicano le regole di utilizzo previste dal presente regolamento, con particolare attenzione alla rimozione di eventuali file elaborati prima della riconsegna.
- 6.3 I PC portatili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.
- 6.4 Tali disposizioni si applicano anche nei confronti di incaricati esterni.
- 6.5 E' vietato connettersi alla rete comunale attraverso qualsiasi dispositivo personale (Pc portatile, smart phone ...) non preventivamente autorizzato dal Servizio S.I.

7. Uso della posta elettronica

- 7.1 **La casella di posta elettronica assegnata all'utente è uno strumento di lavoro.** Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
- 7.2 Le caselle di posta elettronica sono accessibili a tutti i dipendenti comunali specificando, in caratteri minuscoli, un identificativo costituito dalla "**prima lettera del proprio nome**" + "." + "**cognome**" + "**@ceglie.org**" (per es. Mario Rossi accederà con m.rossi@ceglie.org)



- 7.3 È fatto divieto di utilizzare le caselle di posta elettronica per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per:
- l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es.mp3) non legati all'attività lavorativa;
 - l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list;
 - la partecipazione a catene telematiche. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.
- 7.4 La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.
- 7.5 È obbligatorio porre la massima attenzione nell'aprire i file allegati alle e-mail (attachements) prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).
- 7.6 Nel caso in cui un utente di posta si assenti per più giorni (p.es. per malattia), sarà consentito al superiore gerarchico dell'utente o comunque, sentito l'utente, a persona individuata dall'Ente, accedere alla casella di posta elettronica, al fine di garantire la continuità del Servizio lavorativo e comunque nel rispetto del principio di necessità e di proporzionalità.
- 7.7 Il personale del servizio S.I., nell'impossibilità di procedere come sopra indicato e nella necessità di non pregiudicare la necessaria tempestività ed efficacia dell'intervento, potrà accedere alla casella di posta elettronica per le sole finalità indicate al punto 2.3.

8. Navigazione in Internet

- 8.1 **Il PC assegnato al dipendente ed abilitato alla navigazione in Internet costituisce uno strumento utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa.** È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa all'interno dell'Ente.
- 8.2 In questo senso, a titolo puramente esemplificativo, **l'utente non potrà utilizzare Internet** per:
- l'upload o il download di software gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa (filmati e musica) e previa verifica dell'attendibilità dei siti in questione (nel caso di dubbio, dovrà venir a tal fine contattato il personale del Servizio S.I.);
 - l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dalla Direzione Generale (o eventualmente dal Responsabile d'ufficio e/o del Servizio S.I.) e comunque nel rispetto delle normali procedure di acquisto;
 - ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
 - la partecipazione a Forum non professionali, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati dal Responsabile d'ufficio;
 - l'accesso, tramite internet, a caselle web-mail di posta elettronica personale.



- 8.3 Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, *il Comune di Ceglie Messapica* rende peraltro nota l'adozione di uno specifico sistema di blocco o filtro automatico che impedirà determinate operazioni quali l'upload o l'accesso a determinati siti inseriti in una black list.
- 8.4 Gli eventuali controlli, compiuti dal personale incaricato del Servizio S.I. ai sensi del precedente punto 3.3, 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 non oltre 1 mese, ossia il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'Ente.

9. Protezione antivirus

- 9.1 Il sistema informatico del Comune di Ceglie Messapica è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico mediante virus o mediante ogni altro software aggressivo.
- 9.2 Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer nonché segnalare prontamente l'accaduto al personale del Servizio Informatico.
- 9.3 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 prontamente consegnato al personale del Servizio Informatico.

10. Utilizzo dei telefoni, fax e fotocopiatrici aziendali

- 10.1 **Il telefono eventualmente affidato all'utente è uno strumento di lavoro.** Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti l'attività lavorativa stessa. La ricezione o l'effettuazione di telefonate personali è consentito solo nel caso di comprovata necessità ed urgenza.
- 10.2 Qualora venisse assegnato un cellulare aziendale al dipendente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Al cellulare si applicano le medesime regole sopra previste per l'utilizzo del telefono aziendale: in particolare è vietato l'utilizzo del telefono cellulare messo a disposizione per inviare o ricevere SMS o MMS di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa. L'eventuale uso promiscuo (anche per fini personali) del telefono cellulare è possibile soltanto in presenza di preventiva autorizzazione scritta e in conformità delle istruzioni al riguardo impartite dal Direttore generale.
- 10.3 È vietato l'utilizzo dei fax per fini personali, tanto per spedire quanto per ricevere documentazione, salva diversa esplicita autorizzazione da parte del Responsabile di Area.
- 10.4 È vietato l'utilizzo delle fotocopiatrici per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Responsabile di Settore.

11. Osservanza delle disposizioni in materia di Privacy



- 11.1 È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, come indicato nella lettera di designazione ad incaricato del trattamento dei dati ai sensi del Disciplinary tecnico allegato al D.Lgs. n. 196/2003.

12. Accesso ai dati trattati dall'utente

- 12.1 Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.) o per finalità di controllo e programmazione dei costi (ad esempio, verifica costi di connessione ad internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà della Amministrazione, tramite il personale del Servizio S.I. o addetti alla manutenzione, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici aziendali e ai documenti ivi contenuti, nonché ai tabulati del traffico telematico.

13. Sistemi di controlli graduali

- 13.1 In caso di anomalie, il personale incaricato del servizio S.I. effettuerà controlli anonimi che si concluderanno con avvisi generalizzati diretti ai dipendenti del settore in cui è stata rilevata l'anomalia, si evidenzierà l'utilizzo irregolare degli strumenti informatici e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. Controlli su base individuale potranno essere compiuti solo in caso di successive ulteriori anomalie.
- 13.2 In alcun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

14. Sanzioni

- 14.1 È fatto obbligo a tutti i dipendenti di osservare le disposizioni portate a conoscenza con il presente regolamento. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dalla vigente normativa, nonché con tutte le azioni civili e penali consentite.

15. Aggiornamento e revisione

- 15.1 Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate al presente Regolamento. Le proposte verranno esaminate dai Responsabili di Area ed inoltrate al Responsabile Servizio Informatico.

16. Entrata in vigore del regolamento e pubblicità

Con l'entrata in vigore del presente Regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi sostituite dalle presenti.

Copia del regolamento verrà consegnata a ciascun Responsabile di Area per renderlo noto ai rispettivi dipendenti, nonché affisso in modo permanente in luogo visibile a tutti i dipendenti e pubblicato sul sito internet del Comune.