

COMUNE DI MEOLO

Provincia di Venezia



DIRETTIVE PER L'ACCESSO E L'UTILIZZO DEI SERVIZI AZIENDALI DI INTERNET, DI
POSTA ELETTRONICA, DEI FAX, DEI TELEFONI E DELLE STAMPANTI

Indice

Premessa	pag. 2
Art. 1 Definizioni	pag. 3
Art. 2 Entrata in vigore del regolamento e pubblicità	pag. 3
Art. 3 Campo di applicazione del regolamento	pag. 3
Art. 4 Utilizzo del Personal Computer	pag. 3
Art. 5 Gestione ed assegnazione delle credenziali di autenticazione	pag. 5
Art. 6 Utilizzo della rete del Comune	pag. 5
Art. 7 Utilizzo e conservazione dei supporti rimovibili	pag. 6
Art. 8 Utilizzo di PC portatili	pag. 6
Art. 9 Uso della posta elettronica	pag. 6
Art. 10 Navigazione in Internet	pag. 7
Art. 11 Protezione antivirus	pag. 8
Art. 12 Utilizzo dei telefoni, fax e fotocopiatrici aziendali	pag. 8
Art. 13 Osservanza delle disposizioni in materia di Privacy	pag. 9
Art. 14 Accesso ai dati trattati dall'utente	pag. 9
Art. 15 Sistema di controlli gradualmente	pag. 9
Art. 16 Sanzioni	pag. 9
Art. 17 Aggiornamento e revisione	pag. 10
Art. 18 Disposizioni finali	pag. 10

Premessa

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete Internet dai Personal Computer, espone il Comune di Meolo e gli utenti (dipendenti e collaboratori) 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 del Comune stesso.

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 ha adottato delle direttive interne dirette ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

Considerato inoltre che il Comune di Meolo, nell'ottica di uno svolgimento proficuo e più agevole della propria attività, ha messo a disposizione dei propri collaboratori, in relazione al tipo di funzioni svolte, telefoni e mezzi di comunicazione efficienti (computer, telefoni cellulari, etc.), sono state inserite nelle direttive alcune clausole relative alle modalità ed i doveri che ciascun collaboratore deve osservare nell'utilizzo di tale strumentazione.

ART. 1. Definizioni.

Ai fini dell'applicazione delle norme delle direttive si intende

- a) Comune: L'Amministrazione Comunale di Meolo;
- b) C.E.D. (Centro Elaborazione Dati) Il Servizio (interno o esterno in base alle decisioni dell'Amministrazione) che si occupa della gestione delle risorse informatiche e tecnologiche ITC (Information and Communication Tecnology) in dotazione al Comune di Meolo
- c) Utente: ogni dipendente e collaboratore (co.co.co, in stage, ecc.) in possesso di specifiche credenziali di autenticazione. Tale figura potrà anche venir indicata quale "incaricato del trattamento".
- d) Credenziali di autenticazione: Il nome utente e la password che consentono l'accesso al sistema

ART. 2 Entrata in vigore delle direttive e pubblicità

2.1 Le nuove direttive entreranno in vigore il 1° gennaio 2016. Con l'entrata in vigore delle presenti direttive tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti. Sono fatte salve le disposizioni del Documento programmatico della Sicurezza

2.2 Copia delle direttive, oltre ad essere pubblicate sul sito web del Comune di Meolo, verranno consegnate a ciascun dipendente.

ART. 3. Campo di applicazione del regolamento

3.1 Le nuove direttive si applicano 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 coordinati e continuativi, in stage, amministratori ecc.).

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 è vietato, salvo quanto previsto ai successivi punti, 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.

4.2 Il personal computer dato in affidamento all'utente permette l'accesso alla rete del Comune di Meolo solo attraverso specifiche credenziali di autenticazione come meglio descritto al successivo punto 5 delle presenti direttive.

4.3 Il Comune rende noto che il personale incaricato del Servizio CED è stato autorizzato a compiere interventi nel sistema informatico aziendale 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 nn. 9.2 e 10.1, 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 dell'Ente, si applica anche in caso di assenza prolungata od impedimento dell'utente.

4.4 Il personale incaricato del Servizio CED 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 esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In questo ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.

4.5 Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal personale del CED o di altra ditta autorizzata dal CED stesso, 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. Diversamente per esigenze specifiche di determinati uffici/settori potrà essere inoltrata richiesta specifica al Servizio CED indicando o la tipologia di software necessaria o l'esatta denominazione del prodotto richiesto affinché ne possa essere, valutata la compatibilità con le risorse hardware o gli eventuali necessari adeguamenti/alternative che permettano di soddisfare le richieste del settore/ufficio.

4.6 L'inosservanza del primo comma della presente disposizione espone gli inadempienti a gravi responsabilità disciplinari; 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.

Salvo preventiva espressa autorizzazione del personale del Servizio CED non è consentito all'utente modificare le caratteristiche impostate sul proprio PC né procedere ad installare, senza autorizzazione del servizio stesso dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, chiavi usb etc..). È fatta salva la possibilità di individuare, su indicazione del Servizio CED, l'attuazione di soluzioni alternative.

4.7 Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale del Servizio CED nel caso in cui siano rilevati virus ed adottando le procedure previste dal successivo punto 11 delle presenti direttive relative alla protezione antivirus.

4.8 Il Personal Computer deve essere spento al termine dell'orario di lavoro prima di lasciare gli uffici 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.

ART. 5. Gestione ed assegnazione delle credenziali di autenticazione

5.1 Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dal personale del Servizio CED, previa formale richiesta del Responsabile del settore nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente.

5.2 Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), assegnato dal Servizio CED, 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 della password di accensione (bios), senza preventiva autorizzazione da parte del Servizio CED.

5.3 La parola chiave, 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.

5.4 È necessario procedere alla modifica della parola chiave a cura dell'utente, incaricato del trattamento, al primo utilizzo e, successivamente, almeno ogni sei mesi. Ogni tre mesi nel caso invece di trattamento di dati sensibili attraverso l'ausilio di strumenti elettronici.

5.5 Qualora la parola chiave dovesse essere dimenticata sarà sostituita, si procederà in tal senso d'intesa con il personale del Servizio CED, l'utente procederà alla modifica della parola chiave al primo utilizzo.

5.6 Soggetto preposto alla custodia dei criteri di autenticazione è il Referente del Servizio Informatico del Comune.

ART. 6. Utilizzo della rete del Comune

6.1 Per l'accesso alla rete del Comune ciascun utente deve essere in possesso della specifica credenziale di autenticazione.

6.2 È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato. Le parola chiave d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.

6.3 Le cartelle utenti presenti nei server del Comune 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. Sulle stesse vengono svolte regolari attività di controllo, amministrazione e backup da parte del personale del Servizio CED.

6.4 Il personale del Servizio CED 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.

6.5 Risulta opportuno che, con regolare periodicità (almeno ogni sei 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.

ART. 7. Utilizzo e conservazione dei supporti rimovibili

7.1 Tutti i supporti magnetici rimovibili (dischetti, CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati sensibili nonché informazioni riservate dell'Ente, 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 rimovibili contenenti dati sensibili, ciascun utente dovrà contattare il personale del Servizio CED e seguire le istruzioni da questo impartite.

7.3 In ogni caso, i supporti magnetici contenenti dati sensibili devono essere dagli utenti adeguatamente custoditi in armadi chiusi.

7.4 E' vietato l'utilizzo di supporti rimovibili personali.

7.5 L'utente è responsabile della custodia dei supporti e dei dati aziendali in essi contenuti.

ART. 8. Utilizzo di PC portatili

8.1 L'utente è responsabile del PC portatile assegnatogli dal Servizio CED e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

8.2 Ai PC portatili si applicano le regole di utilizzo previste dalle presenti direttive, con particolare attenzione alla rimozione di eventuali file elaborati prima della riconsegna.

8.3 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.

ART. 9. Uso della posta elettronica

9.1 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

9.2 È fatto divieto di utilizzare le caselle di posta elettronica assegnate dal Servizio CED 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 (cd di "Sant'Antonio"). Se si dovessero peraltro ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al personale del Servizio CED. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.

9.3 La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

9.4 Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per il Comune ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analogha dicitura, deve essere visionata od autorizzata dal Responsabile del settore.

9.5 È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario.

9.6 È obbligatorio porre la massima **attenzione nell'aprire i file attachments di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).**

9.7 Al fine di ribadire agli interlocutori la natura esclusivamente aziendale della casella di posta elettronica, i messaggi devono contenere un avvertimento standardizzato nel quale sia dichiarata la natura non personale dei messaggi stessi precisando che, pertanto, il personale debitamente incaricato del Servizio CED potrà accedere al contenuto del messaggio inviato alla stessa casella secondo le regole fissate nella propria policy aziendale.

ART. 10. Navigazione in Internet

10.1. Il PC assegnato al singolo utente ed abilitato alla navigazione in Internet costituisce uno strumento aziendale 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, salvo quanto più sotto precisato.

10.2 In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare internet per:

a) 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 CED);

b) 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 dal Responsabile di settore e/o u.o o del Servizio CED e comunque nel rispetto delle normali procedure di acquisto e negli orari indicati al successivo punto 10.2 d);

c) 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 (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati dal Responsabile d'ufficio;

d) accesso, tramite internet, a caselle web mail di posta elettronica personale durante l'orario di lavoro.

E' consentito all'utente di accedervi nella pausa pranzo, 15 minuti prima di timbrare l'entrata in servizio e nella prima ora successiva al termine dell'orario di lavoro giornaliero.

Ricorrendo tali casi, l'utente dovrà comunque porre la massima attenzione nell'aprire i file attachments di posta elettronica prima del loro utilizzo).

10.3 Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, il Comune rende noto peraltro che potrà attivare 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.

10.4 Gli eventuali controlli, compiuti dal personale incaricato del Servizio CED ai sensi del precedente punto 4.3, potranno avvenire mediante un sistema di controllo dei contenuti o mediante "file di log" della navigazione svolta. Il controllo sui file di log non è continuativo ed i file stessi vengono conservati in base a quanto stabilito dalle vigenti normative legislative e regolamentari in materia. Il periodo di conservazione dei file di log non supererà, comunque, il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'Ente.

ART. 11. Protezione antivirus

11.1 Il sistema informatico del Comune è protetto da software antivirus aggiornato quotidianamente.

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

11.2 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 CED.

11.3 Ogni dispositivo magnetico di provenienza esterna all'Azienda 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 CED.

ART. 12. Utilizzo dei telefoni, fax e fotocopiatrici aziendali

12.1 Il telefono aziendale (fisso e/o mobile) 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.

12.2 Qualora venisse assegnato un cellulare aziendale all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Al cellulare aziendale 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.

12.3 È vietato l'utilizzo dei fax aziendali per fini personali, tanto per spedire quanto per ricevere documentazione, salva diversa esplicita autorizzazione da parte del Responsabile dell'u.o. di appartenenza.

12.4 È vietato l'utilizzo delle fotocopiatrici aziendali per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Responsabile dell'u.o. di appartenenza.

ART. 13. Osservanza delle disposizioni in materia di Privacy

13.1 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 Disciplinare tecnico allegato al D.Lgs. n. 196/2003.

ART. 14. Accesso ai dati trattati dall'utente

14.1 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 aziendali (ad esempio, verifica costi di connessione ad internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà dell'Amministrazione Comunale, tramite il personale del Servizio CED 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 telefonico.

ART. 15. Sistemi di controlli gradualità

15.1 In caso di anomalie, il personale incaricato del Servizio CED effettuerà controlli anonimi che si concluderanno con avvisi generalizzati diretti ai dipendenti dell'u.o. 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. Controlli su base individuale potranno essere compiuti solo in caso di successive ulteriori anomalie.

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

ART. 16. Sanzioni

16.1 È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con le presenti direttive. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dal vigente CCNL del comparto Regioni/Autonomie Locali e dalle vigenti norme legislative in materia, nonché con tutte le azioni civili e penali consentite.

ART. 17. Aggiornamento e revisione

17.1 Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate alle presenti direttive. Le proposte verranno esaminate congiuntamente dal Segretario Generale e dal personale incaricato del Servizio CED.

17.2 Le direttive sono soggette a revisione con frequenza triennale o, più frequente, qualora sia richiesto da modifiche e novità legislative intervenute in materia.

ART. 18 Disposizioni Finali.

18.1 Le presenti direttive disciplinano l'utilizzo dei sistemi e delle risorse informatiche del Comune ed è rilevante solamente ai fini disciplinari e pertanto non deroga in alcun modo a quanto previsto nel Documento programmatico sulla sicurezza.