COMUNE DI MONTA'
Provincia di Cuneo

DISCIPLINARE SULL 'UTILIZZO DEGLI STRUMENTI INFORMATICI

Premessa

Il Comune di Montà riconosce l'importanza assunta dagli strumenti informatici e telematici nell'organizzazione del lavoro, caratterizzando l'azione amministrativa per una maggiore efficacia ed efficienza.

Nonostante l'indubbia semplificazione amministrativa, l'utilizzo improprio delle tecnologie, anche se inconsapevole, pone in pericolo le infrastrutture stesse, le informazioni ed i dati ivi contenuti.

L'utilizzo non corretto degli strumenti informatici può comportare anche la lesione della riservatezza dei dipendenti, degli amministratori o dei terzi. L'azione amministrativa comporta infatti il trattamento di dati personali, alcuni dei quali potrebbero toccare la vita privata o la sfera più personale. L'Amministrazione promuove quindi ogni opportuna misura, organizzativa e tecnologica, volta a prevenire il rischio di utilizzi impropri delle strumentazioni e delle banche dati del Comune.

Per quanto non specificato nel presente documento è richiesto comunque un atteggiamento ispirato alla correttezza ed alla buona fede.

Capo I – Finalità, ambito di applicazione e principi generali

Art. 1 – Finalità

1. Il presente disciplinare è finalizzato a definire le modalità di accesso ed utilizzo degli strumenti informatici, della rete informatica e telematica e dei servizi che tramite la stessa rete è possibile ricevere all'interno e all'esterno dell'Amministrazione, ai fini di un corretto utilizzo degli strumenti stessi da parte di amministratori, dipendenti dell'Ente o collaboratori, consulenti, stagisti, tirocinanti e soggetti autorizzati dal Comune (di seguito «utenti»).

2. Ulteriore obiettivo è rappresentato dalla volontà di preservare il diritto alla riservatezza degli utenti interni od esterni alla rete informatica e telematica

3. Si intende inoltre responsabilizzare gli utilizzatori sulle conseguenze di un uso improprio delle predette strumentazioni.

4. Per quanto non espressamente previsto dal presente atto, si fa rinvio alle disposizioni generali vigenti in materia.

Art. 2 – Ambito di applicazione

1. La rete del Comune Montà è costituita dall'insieme delle risorse informatiche, cioè dalle risorse hardware e software, e dal patrimonio informativo digitale.
2. Il patrimonio informativo è l'insieme delle banche dati in formato digitale ed in generale tutti i documenti prodotti tramite l'utilizzo dei suddetti apparati.

3. Il presente disciplinare si applica a tutti gli utenti autorizzati ad accedere alle risorse tecnologiche del sistema informatico del Comune o comunque nella disponibilità dell'Ente.

Art. 3 – Principi generali

1. Il Comune di promuove l'utilizzo della rete informatica e telematica, di internet e della posta elettronica quali strumenti utili a perseguire con efficacia ed efficienza le proprie finalità istituzionali, in accordo con le linee guida ed i principi delineati dalla normativa vigente.

2. Ogni utente è responsabile, civilmente e penalmente, del corretto uso delle risorse informatiche, dei servizi/programmi a cui ha accesso e dei dati trattati a fini istituzionali. È altresì responsabile del contenuto delle comunicazioni effettuate e ricevute a fini istituzionali anche per quanto attiene la riservatezza dei dati ivi contenuti, la cui diffusione impropria potrebbe configurare violazione del segreto d'ufficio o della normativa per la tutela dei dati personali

3. Il lavoratore deve custodire ed utilizzare gli strumenti informatici, internet, la posta elettronica in modo appropriato e diligente ed è responsabile della propria postazione di lavoro.

4. Sono vietati comportamenti che possono creare un danno, anche d'immagine, all'Ente.

Capo II – Criteri di utilizzo degli strumenti informatici e telematici

Art. 4 – Utilizzo degli strumenti informatici

1. Gli strumenti informatici (a titolo esemplificativo personal computer, stampante) messi a disposizione degli utenti, costituiscono strumento di lavoro. Pertanto l'utilizzo di essi da parte degli utenti è consentito per finalità attinenti o comunque connesse con l'attività lavorativa, secondo criteri di correttezza e professionalità, coerentemente al tipo di attività svolta e nel rispetto delle disposizioni normative ed interne e delle esigenze di funzionalità e di sicurezza dei sistemi informativi.

2. Nella definizione di attività lavorativa sono comprese anche le attività strumentali e collegate alla stessa, quali ad esempio quelle che attengono allo svolgimento del rapporto di lavoro. E' escluso qualsivoglia uso per scopi privati e/o personali, ad eccezione dei casi d'urgenza e comunque a condizione che tale uso avvenga in modo non ripetuto o per periodi prolungati.

Art. 5 – Utilizzo del personal computer

1. L'accesso alla stazione di lavoro è condizionato al corretto inserimento delle credenziali di autenticazione (nome utente e password). Per l'uso, la scelta, la modifica e la custodia delle credenziali si rinvia a quanto previsto dalla scheda tecnica.+

2. Il personal computer assegnato come postazione di lavoro è configurato con il software necessario al suo utilizzo. Ogni altra installazione, anche di software gratuito e liberamente scaricabile da internet, deve essere previamente autorizzata così come qualsiasi modifica delle configurazioni hardware

3. Ogni utente deve tenere comportamenti corretti, tali da preservare il buon funzionamento degli strumenti e tali da ridurre i rischi per la sicurezza del sistema informatico, quali l'utilizzo di supporti per la memorizzazione dei dati non sicuri e CD provenienti dall'esterno, al fine di non diffondere virus.

4. E' vietata l'installazione non autorizzata di hardware che consenta l'accesso non controllato all'esterno della rete comunale (a titolo esemplificativo internet key, chiavi Wireless USB o modem che sfruttino il sistema di comunicazione telefonico per l'accesso a internet o a banche dati esterne).

5. E' vietato copiare o mettere a disposizione di altri materiale protetto dalla legge sul diritto di autore (documenti, files musicali, immagini, filmati e simili) di cui l'Ente non abbia acquisito preventivamente i diritti.

6. Gli applicativi gestionali (Gestione, Protocollo, Anagrafe…) sono destinati alla gestione di informazioni il cui utilizzo deve essere compatibile con la disciplina vigente in materia di privacy.

7. Tutti i dati personali, soprattutto quelli di natura particolare, riprodotti su supporti magnetici o su supporti cartacei devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato, facendosi rinvio alla scheda tecnica. Non è pertanto consentito lasciare incustoditi presso le stampanti documenti cartacei contenenti dati particolari.

8. La tutela dei dati archiviati su personal computer che gestiscono localmente documenti e dati è demandata all'utente, il quale dovrà effettuare periodicamente i salvataggi su supporti dedicati ed idonei, nonché la conservazione degli stessi in luoghi adatti.

Art. 6 – Credenziali di accesso

1. L'accesso alle procedure informatiche dell'Ente è consentito agli incaricati in possesso di "credenziali di autenticazione" che permettano il superamento di una procedura di autenticazione e di autorizzazione.

2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato (userid o username) associato ad una parola chiave riservata (password). Possono essere utilizzati, allo scopo, strumenti con livelli di sicurezza superiori, quali dispositivi di autenticazione (es. smartcard) biometrici.

3. Gli incaricati sono responsabili della custodia e dell'utilizzo delle proprie credenziali di autenticazione e devono utilizzarle e gestirle attenendosi alle istruzioni contenute nella scheda tecnica

4. Le credenziali di autenticazione individuali per l'accesso alle applicazioni non devono mai essere condivise tra più utenti. Qualora un utente dovesse avere la necessità di trattare dati o usare le procedure, il dirigente o il responsabile del servizio di riferimento potrà richiedere formalmente al Responsabile dei Sistemi Informatici, le relative credenziali di autenticazione, dotate dei privilegi necessari all'accesso ai dati o ai servizi richiesti.

Art. 7 – Utilizzo della rete comunale

1. Le unità di rete 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. Su queste unità vengono svolte regolari attività di controllo, amministrazione e backup da parte dell'Ufficio Informatica.

2. Il Comune può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà pericolosa per la sicurezza sia sui PC degli incaricati sia sulle unità di rete.

3. 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' infatti da evitare un'archiviazione ridondante.

Art. 8 – Utilizzo della rete internet

1. L'accesso alla Rete Internet costituisce strumento di lavoro ed è consentito per finalità direttamente attinenti o comunque connesse all'esercizio dell'attività lavorativa. E' escluso qualsivoglia uso per scopi privati e/o personali, salvo che tale uso sia motivato da ragioni di urgenza o di necessità. E' in ogni caso vietato l'uso reiterato e prolungato per fini personali.

2. L'Amministrazione adotta misure di filtraggio che permettono di inibire o restringere l'accesso a siti i cui contenuti siano classificati pericolosi o non attinenti agli scopi istituzionali oppure che permettono l'accesso solo a determinati siti la cui consultazione sia stata ritenuta dai singoli Responsabili Informatici utile in relazione agli scopi istituzionali.

3. Sono vietate azioni idonee ad eludere le misure di filtraggio di cui al precedente comma.

4. È altresì fermamente vietato:

    a) scaricare e/o installare software non espressamente autorizzati dal Comune;
    b) scaricare e/o usare materiale informatico non direttamente attinenti all'esercizio della attività lavorativa;
    c) scaricare e/o usare materiale informatico il cui contenuto (a mero titolo esemplificativo: software, testo, audio e video) sia coperto da diritto di autore. Nei casi in cui ciò sia necessario per lo svolgimento dell'attività lavorativa, l'utente è tenuto ad attivare preventivamente gli adempimenti previsti dalla legge;
    d)) partecipare a forum di discussione on line, a chat, utilizzare sistemi di chiamata o di

video chiamata, ecc. per ragioni non direttamente attinenti o connesse all'attività lavorativa;

e) navigare in internet su siti contrari a norme di legge;
f) effettuare ogni genere di transazione finanziaria per fini personali;
g) installare e utilizzare strumenti per lo scambio di dati attraverso internet con metodologia
PEER to PEER (es.eMule, kazaa, bittorrent etc.) indipendentemente dal contenuto dei file scambiati;
h) usare i profili social del Comune per fini personali, politici o commerciali;
i) utilizzare i profili personali attivati sui social media per agire in nome e per conto del Comune

5. Per esigenze di sicurezza delle informazioni dell'ente e per le attività di tutela che gli sono proprie, qualora si ravvisi un traffico anomalo o accessi a siti non connessi ad attività istituzionali o in grado di generare eventi dannosi o situazioni di pericolo o di disfunzioni operative per il Comune di, il dirigente competente può autorizzare il funzionario Responsabile dei Sistemi Informatici ad individuarne le cause e l'origine.

Art. 9 – Utilizzo della posta elettronica

1. Il Comune mette a disposizione di ogni utente il servizio di posta elettronica, assegnando a ciascuno di essi caselle di posta istituzionali per fini esclusivamente lavorativi.

2. Al fine di agevolare lo svolgimento dell'attività lavorativa, il Comune rende disponibili indirizzi di posta elettronica condivisi tra più utenti (caselle di posta istituite per singole unità organizzative) affiancandoli a quelli individuali.

3. L'indirizzo di posta elettronica messa a disposizione dal Comune, contraddistinto dalla presenza del nome di dominio "comune.it", costituisce uno strumento di lavoro ed il suo utilizzo è consentito unicamente per finalità attinenti o comunque connesse allo svolgimento dell'attività lavorativa.

4. E' escluso l'uso per scopi privati e/o personali, ad eccezione dei casi d'urgenza e di necessità e comunque non in modo ripetuto.

5. La sicurezza e la riservatezza della posta elettronica sono garantite dalla necessità di disporre di idonee credenziali di autenticazione per accedere alla stessa. La password dell'account di posta elettronica è scelta e registrata dall'incaricato nel rispetto dei criteri e delle regole indicati nella scheda tecnica in materia di misure minime di sicurezza.

6. E' fatto divieto di:

a) inviare o memorizzare messaggi di natura oltraggiosa, volgare, diffamatoria e/o discriminatoria, ed in ogni caso contrari a norme di legge o idonei a creare danno al Comune o a terzi; nonché messaggi a catena e/o spam ;
b) scambiare messaggi impersonando un mittente diverso da quello reale;
c) scambiare messaggi di posta contenenti file o link a siti con contenuti illegali, violenti, o pornografici, file o materiale informatico soggetto al diritto d'autore, password e/o codici d'accesso a programmi soggetti a diritto d'autore e/o a siti internet;
d) aprire messaggi di posta o allegati di tipo eseguibile, salvo il caso di certezza assoluta dell'identità del mittente e della sicurezza del messaggio;
e) inviare, anche da una casella di posta privata, messaggi di natura personale e non

attinenti al rapporto di lavoro a indirizzi di posta elettronica contraddistinti dal dominio “comune.it”.

7. Il responsabile del servizio, qualora rilevi un utilizzo improprio della posta elettronica da parte di un utente o comunque una violazione delle regole e dei divieti di cui al presente Disciplinare, ne informa l'utente interessato che potrà chiedere di essere ascoltato e di accedere alla relativa documentazione. A seguito delle verifiche effettuate, il dirigente di settore avvia, se del caso, i procedimenti conseguenti.

Capo IV – Controlli

Art. 10 – Controlli e responsabilità

1. L’Amministrazione si riserva di effettuare controlli sul corretto utilizzo degli strumenti informatici e telematici nel rispetto dei principi di pertinenza e non eccedenza, di correttezza e di gradualità come previsto dalla normativa vigente.

2. Per esigenze organizzative, produttive e di sicurezza l’Amministrazione può avvalersi di strumenti che consentono un controllo a distanza di tipo generalizzato, indiretto e anonimo, relativo all’intera struttura amministrativa, ad aree, settori o gruppi di utenti. I controlli possono essere attivati dall’Ufficio Informatica a seguito di richiesta del responsabile del servizio o a seguito della rilevazione di anomalie / malfunzionamenti del sistema. Il primo controllo sarà anonimo e nel rispetto del principio di gradualità; qualora – durante un controllo generalizzato – vengano rilevate anomalie nell’utilizzo degli strumenti informatici, l’Ente procede preliminarmente all’invio di un avviso generalizzato relativo all’uso improprio riscontrato, con l’invito ad attenersi scrupolosamente al presente Regolamento, e riservandosi la facoltà di svolgere successive azioni mirate alla verifica del corretto utilizzo.

3. Il mancato rispetto o la violazione delle norme contenute nel presente Regolamento è perseguibile con provvedimenti disciplinari, nonché con le azioni civili e penali consentite.

Art. 11 – Responsabilità degli utenti

1. L'utente non può in alcun caso modificare la configurazione di rete e non può effettuare manomissioni o interventi sulle apparecchiature o sui programmi non formalmente autorizzati dall’Ufficio Informatica, al quale deve comunicare tempestivamente le necessità di interventi su apparecchiature e programmi in ordine alla corretta prestazione dei serviz

2. L'accesso alla risorsa informatica è personale e va effettuato tramite nome utente e password di identificazione. L’accesso non può essere condiviso o ceduto.Gli utenti sono responsabili per la protezione dei dati utilizzati e/o memorizzati nei sistemi in cui hanno accesso; è fatto loro divieto di accedere direttamente o indirettamente a directory, files e servizi non espressamente e preventivamente autorizzati dall’Ente.

3. La password è personale e non cedibile o trasmissibile a terzi: è fatto divieto a ciascun utente di divulgare, per fatto imputabile a lui direttamente o indirettamente, password, username e comunque chiavi di accesso riservate. Se smarrite, va fatta immediata segnalazione e richiesta di sostituzione all’Ufficio Informatica, fatto salvo quanto previsto all’art. 7, comma 4.

4. Gli utenti sono obbligati a segnalare immediatamente all'Ufficio Informatica ogni sospetto di effrazione, incidente, abuso o violazione della sicurezza.

5. Gli utenti sono tenuti a mantenersi aggiornati, controllando periodicamente le direttive dell'Ufficio Informatica divulgate tramite e-mail.

Capo – Disposizioni finali

Art. 12 - Violazioni

1. Il dipendente deve attenersi, nell'utilizzo e nella gestione delle risorse strumentali informatiche comunali, oltre che alle norme del presente Regolamento, ai principi e ai doveri stabiliti nel "Codice di comportamento dei dipendenti delle pubbliche amministrazioni".

2. La violazione da parte dei lavoratori dei principi e delle norme 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.

SCHEDA TECNICA

(allegata al "Disciplinare per l'utilizzo degli strumenti informatici, di internet e della posta elettronica da parte dei dipendenti")

1. Il trattamento dei dati personali avviene previo superamento di una procedura di autenticazione.
2. Ciascun incaricato ha un codice per l'identificazione (o un *username*) associato a una parola chiave riservata conosciuta solamente dal medesimo; in alternativa, l'incaricato ha un dispositivo di autenticazione in suo esclusivo possesso ed uso, eventualmente associato a un codice identificativo o a una parola chiave; oppure per il superamento della procedura di autenticazione potrà essere usata una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o ad una *password*.
3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.
4. Sarà cura dell'incaricato adottare le necessarie cautele per assicurare la segretezza delle credenziali nonché la diligente custodia dei dispositivi in suo esclusivo possesso o uso. La parola chiave deve essere custodita con la massima attenzione e segretezza e non deve essere divulgata o comunicata a terzi. La parola chiave non deve essere scritta su nessun tipo di supporto (cartaceo, elettronico, ecc.). L'utente è responsabile di ogni utilizzo indebito o non consentito delle credenziali di autenticazione di cui sia titolare.
5. La *password*, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, con cadenza periodica (si consiglia almeno ogni sei mesi); è opportuno che la parola chiave contenga lettere, numeri e caratteri c.d. speciali. In caso di trattamento di categorie particolari di dati la password è modificata secondo una più breve periodicità.
6. Nello scegliere la propria password, si devono utilizzare anche caratteri speciali, numeri, lettere maiuscole e minuscole. Non si devono scegliere come password parole presenti in un dizionario, sia della lingua italiana che di lingue straniere, nè utilizzare parole ottenute come combinazione di tasti vicini sulla tastiera o sequenze di caratteri (ad esempio *qwerty, asdfgh, 123321, aabbcc,* ecc.).
7. Il codice per l'identificazione, laddove utilizzato, è univoco e non può essere assegnato ad altri incaricati, neppure in tempi diversi.
8. Le credenziali di autenticazione non utilizzate da almeno sei mesi, se possibile, sono disattivate. Sono inoltre disattivate in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali;
9. Durante una sessione di trattamento l'incaricato non deve lasciare incustodito e accessibile lo strumento elettronico. È opportuno effettuare il *log-out* dal sistema quando ci si assenta, anche momentaneamente.
10. I dati informatici devono essere conservati in archivi protetti da *username*, PIN o *password* di resistenza e custodia idonea.
11. I sistemi informatici devono essere adeguatamente protetti da antivirus, firewall ed altri strumenti idonei a proteggere adeguatamente i sistemi informatici.
12. I supporti rimovibili contenenti dati personali devono essere adeguatamente custoditi.
13. Al fine di evitare perdite di dati conservati per ragioni d'ufficio, è opportuno provvedere ad un periodico backup dei dati stessi secondo gli stessi standard di sicurezza di cui ai precedenti punti.

14. La sicurezza degli apparati informatici non può prescindere dal costante aggiornamento del sistema operativo e dei software gestionali
15. Si devono prevedere adeguate misure antincendio relativamente ai locali dove alloggiano le apparecchiature.

N.B. : per quanto non espressamente indicato nella presente scheda tecnica e per ogni forma di approfondimento di dettaglio, si fa rinvio al testo integrale del Disciplinare