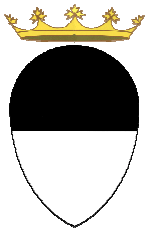

COMUNE DI FERRARA

DISCIPLINARE INTERNO PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI E TELEMATICI MESSI A DISPOSIZIONE DALL'AMMINISTRAZIONE COMUNALE

INDICE

1. FINALITÀ 3

2. AMBITO DI APPLICAZIONE 3

3. PRINCIPI GENERALI 3

4. UTILIZZO DEL PERSONAL COMPUTER 4

5.USO DI PC PORTATILI E ALTRE APPARECCHIATURE MOBILI 7

6. UTILIZZO DELLE STAMPANTI E DEI MATERIALI DI CONSUMO 8

7. GESTIONE DELLE PASSWORD E DEGLI ACCOUNT 8

8. PROFILI DI AUTORIZZAZIONE ED UTILIZZO DELLA RETE 8

9. USO DELLA POSTA ELETTRONICA 9

10. USO DELLA RETE INTERNET E DEI RELATIVI SERVIZI 10

11. PROTEZIONE ANTIVIRUS. 10

12. MANCATA OSSERVANZA DEL DISCIPLINARE 11

13. CONTROLLI E VERIFICHE 11

ALLEGATO A - GLOSSARIO DEI TERMINI TECNICI E INFORMATICI 14

Premessa
Negli ultimi anni l'organizzazione del lavoro è stata sottoposta ad un imponente processo di informatizzazione e, in tale contesto, i servizi di rete, tra cui posta elettronica e Internet, sono diventati strumenti quotidiani indispensabili per l'esercizio dell'attività lavorativa. Tuttavia l'uso di tali strumenti in maniera non corretta, anche a seguito di comportamenti inconsapevoli, può essere causa di gravi minacce e problemi per la sicurezza del sistema e delle informazioni in esso contenute. A ciò aggiungasi che le informazioni trattate nell'ambito dell'attività lavorativa possono riguardare la sfera personale e la vita privata dei lavoratori e di terzi per cui le attività di monitoraggio cui possono essere sottoposte le risorse informatiche messe a disposizione sia del personale dell'Ente che ai fornitori esterni dovranno sempre ispirarsi al rispetto della normativa sulla tutela della riservatezza dei dati personali nonché ai ***principi di diligenza e correttezza***.

1. Finalità
Il presente disciplinare, quindi, persegue le seguenti finalità:

- adottare indirizzi trasparenti, capaci di comunicare con estrema chiarezza ai lavoratori le corrette modalità di utilizzo degli strumenti informatici assegnatigli per lo svolgimento delle mansioni loro attribuite;

- definire con altrettanta chiarezza il diritto dell'Amministrazione a verificare l'uso corretto dei suddetti strumenti nonchè le modalità con le quali l'Amministrazione esercita tale diritto di verifica.

Per quanto non espressamente previsto dal presente atto, si rinvia alle disposizioni generali vigenti in materia, con particolare riferimento alle ***Linee Guida del Garante per Posta Elettronica e Internet*** (Delib. Garante Privacy n. 13 del 1° marzo 2007), ed alla ***Direttiva della Presidenza del Consiglio dei Ministri - Dipartimento della Funzione Pubblica- n. 2/2009***.

L'Amministrazione comunale è tenuta ad assicurare la funzionalità degli strumenti informatici assegnati ai lavoratori e si impegna a promuovere ogni opportuna misura, organizzativa e tecnologica, volta a prevenire il rischio di utilizzi impropri delle strumentazioni e delle banche dati di proprietà dell'Ente.

2. Ambito di applicazione
La rete del Comune di Ferrara è costituita dall'insieme delle risorse informatiche, cioè dalle risorse infrastrutturali e dal patrimonio informativo digitale.

Le ***risorse infrastrutturali*** sono le componenti hardware/software e gli apparati elettronici collegati alla rete informatica comunale. 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.

Il presente disciplinare si applica a tutti gli utenti che a diverso titolo sono autorizzati ad accedere alla rete comunale. Per **utenti** si intendono gli amministratori, i dirigenti, i dipendenti a tempo indeterminato e determinato, ed i collaboratori impiegati a diverso titolo presso l'amministrazione, compreso il personale fornito da terze parti.

3. Principi generali
Gli strumenti informatici forniti al personale devono essere utilizzati esclusivamente per lo svolgimento del lavoro assegnato con modalità e comportamenti adeguati ai compiti ed alle responsabilità dei dipendenti pubblici,

nel rispetto delle comuni regole previste per la sicurezza dei sistemi informatici e per la tutela dei dati.

Ciascun dipendente è responsabile per l'utilizzo anche da parte di terzi, degli strumenti informatici a lui affidati. Per **strumenti informatici** si intendono: personal computer fissi o portatili, videoterminali, stampanti locali o di rete, i prodotti software regolarmente licenziati, palmari, cellulari o altri dispositivi di telecomunicazione, le relative periferiche nonché tutta l'infrastruttura logica e fisica che permette l'interconnessione delle postazioni di lavoro al fine di agevolare la trasmissione di dati.

Il personale deve custodire la propria strumentazione in modo appropriato e diligente, segnalando tempestivamente ogni danneggiamento, furto o smarrimento al proprio Responsabile di Servizio.

E' tassativamente proibito installare programmi provenienti dall'esterno, in quanto l'utilizzo di software non regolarmente acquistato dall'Ente può configurare un reato ed essere causa di diffusione di virus informatici, oltre a costituire un grave pericolo per la stabilità delle applicazioni dell'elaboratore.

Le aree di memorizzazione condivise in rete, sono spazi di condivisione di informazioni messe a disposizione dall'Ente per lo svolgimento dell'attività lavorativa e non possono in alcun modo essere utilizzate per scopi diversi. Su queste unità, vengono svolte regolari attività di verifica e/o back-up da parte degli addetti al Servizio Sistemi Informativi appositamente incaricati da ciascun Responsabile del trattamento, i quali potranno, in qualunque momento, procedere alla rimozione di ogni file o applicazione che riterranno pericolosi per la sicurezza o non inerenti all'attività lavorativa sia sui PC dei dipendenti sia sulle unità di rete. La stessa facoltà, sempre ai fini di garantire la salvaguardia e la sicurezza del sistema informatico e per ulteriori motivi tecnici e manutentivi, si applica anche in caso di assenza prolungata o impedimento dell'utente.

Costituisce buona regola la periodica pulizia degli archivi, con cancellazione dei files obsoleti o inutili. Particolare attenzione, inoltre, deve essere prestata alla duplicazione dei dati. E', infatti, assolutamente da evitare un'archiviazione ridondante che non consenta in modo chiaro ed inequivocabile, l'identificazione dello stato di revisione di un documento.

L'utilizzo degli strumenti informatici al di fuori dell'orario di servizio è consentito solo previa autorizzazione del proprio Responsabile di Servizio. Infine, il personale è tenuto ad osservare le direttive del Servizio Sistemi Informativi volte a garantire il corretto funzionamento delle procedure di backup le quali possono essere reperite al seguente link:
http://intranet.ssi.fe/index.phtml?id=658

4. Utilizzo del personal computer

Il Comune di Ferrara mette a disposizione dei propri utenti le strumentazioni informatiche necessarie per lo svolgimento delle attività lavorative. Gli stessi diventano responsabili delle strumentazioni durante il loro utilizzo. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione altrimenti non necessari e, soprattutto, minacce alla sicurezza.

Non è consentito all'utente modificare le caratteristiche hardware e software impostate sul proprio Personal Computer (PC), salvo autorizzazione esplicita da parte del Responsabile del Servizio di appartenenza.

Il Personal computer deve essere spento al termine di ogni turno giornaliero di lavoro, prima di lasciare gli uffici, e comunque deve essere protetto nelle pause durante l'orario di lavoro. Pertanto, ogni qualvolta il dipendente si allontani o si assenti dalla postazione di lavoro è tenuto a chiudere la sessione **(Ctrl+Alt+Canc quindi "Blocca Computer")**, oppure a rendere inaccessibile a terzi (ad esempio mediante l'utilizzo del salvaschermo dotato di password) la propria postazione di lavoro. E' evidente che 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.

E' vietato l'uso di dispositivi di memorizzazione removibili scrivibili personali. Gli utenti che necessitino, per ragioni attinenti allo svolgimento dell'attività lavorativa, di utilizzare supporti di memorizzazione removibili devono farne richiesta all'Amministrazione attraverso il proprio Responsabile che dovrà sempre indicare una persona responsabile dell'utilizzo dei dispositivi assegnati. In caso di utilizzo di dispositivi di memorizzazione rimovibili assegnati dall'Amministrazione, l'utente dovrà comunque provvedere alla custodia e all'uso dei medesimi adottando tutti gli accorgimenti necessari per evitare accessi non autorizzati e/o trattamenti non consentiti dei dati in essi contenuti. Egli dovrà in particolare distruggere i dati sul dispositivo al termine del loro utilizzo per evitare la creazione di copie non controllate.

Eventuali dispositivi di memorizzazione rimovibili contenenti dati e informazioni se non utilizzate, dovranno essere distrutti o resi inutilizzabili. Il riutilizzo di tali supporti, invece, potrà essere consentito a soggetti non autorizzati al trattamento di tale tipologia di dati, solo se le informazioni precedentemente in essi contenute non siano più intellegibili e/o tecnicamente in alcun modo ricostruibili.

Per "*dispositivo di memorizzazione rimovibile*" si intende qualunque dispositivo di memorizzazione asportabile o scrivibile che utilizzi supporti rimovibili (nastri, floppy, cd, memorie elettroniche, …).

Tutti i supporti magnetici riutilizzabili (*cd, dischetti, cassette e cartucce*) contenenti dati personali, sia comuni che sensibili, devono essere trattati con particolare cautela. In alcuni casi, infatti, è possibile recuperare i dati memorizzati anche dopo la loro cancellazione. Per questo motivo il supporto, al termine dell'utilizzo, deve essere formattato prima di essere riutilizzato, oppure distrutto.

L'operatore avrà cura di effettuare la stampa di documenti contenenti dati personali solo se strettamente necessaria provvedendo a ritirarli immediatamente dai vassoi delle stampanti condivise. Si dovrà evitare in ogni modo e per quanto possibile, di dislocare stampanti e fax in aree accessibili a soggetti non abilitati al trattamento e non presidiate (per esempio: corridoi aperti al pubblico, sale d'attesa, ecc.).

Le informazioni archiviate informaticamente devono essere esclusivamente quelle previste dalla legge o necessarie all'attività lavorativa dell'ufficio. La tutela della gestione sulle stazioni di lavoro è demandata all'utente che dovrà effettuare, con frequenza opportuna (*secondo le modalità contenute nel* ***Documento Programmatico sulla Sicurezza*****)**, i salvataggi su supporti magnetici e/o di rete e la conservazione degli stessi in luogo idoneo.

Non è consentita l'installazione di programmi diversi da quelli autorizzati dall'Ente. Non è, inoltre, consentita la riproduzione o la duplicazione di programmi informatici.

Si possono effettuare **copie di dati** su supporti rimovibili (*es. dischetti CD, DVD, chiavi usb*) solo se autorizzati da parte del proprio Dirigente. Qualora sulle copie venissero trasferiti dati personali, gli stessi vanno utilizzati con le modalità previste dalla legge, e secondo **il principio di necessità**. Al termine del trattamento sarà cura del dipendente distruggere o rendere inutilizzabili i supporti rimovibili eventualmente utilizzati.

I supporti rimovibili contenenti dati sensibili o giudiziari, se non utilizzati, devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri dipendenti, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e in alcun modo ricostruibili.

Le procedure e istruzioni per la dismissione di materiale informatico sono riportate alla seguente pagina di intranet: http://intranet.ssi.fe/index.phtml?id=279
.
Per rispetto delle norme che regolano la tutela giuridica del software e per la necessità di garantire integrità e stabilità delle applicazioni installate sul personal computer stesso **non è consentito**:

1. **alterare, rimuovere o danneggiare le configurazioni del software e dell'hardware dei personal computer;**
2. **installare e utilizzare programmi informatici che non siano stati ufficialmente forniti o acquistati dall'Ente;**
3. **installare giochi, screensavers non propri del sistema operativo, client chat etc;**
4. **installare dispositivi di comunicazione (*modem*) se non con l'autorizzazione espressa del Responsabile del Servizio Sistemi informativi;**
5. **installare o connettere periferiche proprie;**
6. **scaricare da internet o da supporto magnetico proveniente dall'esterno file di provenienza sconosciuta senza farli sottoporre a opportuno controllo;**
7. **divulgare informazioni tecniche relative alla struttura informatica comunale che possano pregiudicare la sicurezza della stessa.**

E' inoltre vietato:

1. **utilizzare gli strumenti informatici comunali al fine di custodire, far circolare o promuovere materiale pubblicitario personale, codice maligno *(virus, trojan horses, programmi pirata)* e/o altro materiale non autorizzato;**
2. **copiare o mettere a disposizione di altri, materiale protetto dalla legge sul diritto d'autore (*documenti, files musicali, immagini, filmati e simili*) di cui l'ente non abbia acquisito i diritti;**
3. **utilizzare la strumentazione informatica per la realizzazione, redazione, memorizzazione e spedizione di documenti di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione, appartenenza sindacale e politica.**

I **fornitori esterni**, addetti alla manutenzione di hardware, software e reti, operano in conformità alle presenti disposizioni, sotto la sorveglianza dei Responsabili del trattamento.

5. Utilizzo di personal computer portatili e altre apparecchiature mobili

L'Ente può prevedere la consegna, per motivate ragioni d'ufficio, a dipendenti, individualmente identificati, di Personal Computer portatili. Le regole di utilizzo di queste apparecchiature sono le stesse dei PC collegati alla rete locale anche se i servizi disponibili e la loro modalità di erogazione potrebbe differenziarsi dalle postazioni "fisse". Essi devono, comunque, essere custoditi in un luogo protetto. I P.C. portatili che rimangono sconnessi a lungo dalla rete non ricevono gli aggiornamenti automatici e possono avere quindi un livello di protezione non allineato con gli standard dell'Ente. E' quindi a carico dell'utilizzatore garantire la funzionalità e l'aggiornamento del sistema, in modo particolare è necessario aggiornare periodicamente l'Antivirus.

Il PC portatile ha la caratteristica di essere trasportabile con facilità e presenta, quindi, peculiarità in termini di utilizzo e di sicurezza. Per le modalità generali di utilizzo l'utente deve osservare, in quanto applicabili, le regole stabilite dal presente disciplinare in materia di uso del PC.

Il PC portatile non deve essere mai lasciato incustodito, in particolare:

- durante il periodo di permanenza in ufficio deve essere assicurato in modo opportuno
- durante le ore notturne o in periodo di assenza non deve mai essere lasciato sulla scrivania ma deve essere custodito in modo opportuno (es. riposta in armadi chiusi a chiave o portato al seguito).

Durante gli spostamenti all'esterno è cura dell'utente proteggere il PC portatile da possibili furti o danneggiamenti; il dispositivo assegnato non deve mai, nemmeno per breve tempo, rimanere incustodito, soprattutto in luoghi pubblici quali, ad esempio, aeroporti, stazioni ferroviarie, stazioni di servizio, ristoranti, bar, fiere, manifestazioni, etc. Durante i viaggi deve essere sempre trasportato come bagaglio a mano, e non va mai lasciato in vista nelle stanze di hotel, residence, alloggi, etc., bensì deve essere opportunamente richiuso in valigia o in un armadio, o in cassaforte in caso di assenza prolungata.

Ogni utente è responsabile dell'integrità dei dati che conserva "in locale" sul proprio PC portatile, e deve tenere in considerazione il fatto che i dati potrebbero essere persi o compromessi. A tale riguardo l'utente è tenuto a:

- memorizzare in forma protetta (es. accesso al file con password), in modo adeguato al loro livello di criticità o riservatezza, eventuali informazioni riservate/segrete residenti sul PC;
- effettuare, con cadenza quotidiana, durante i periodi lavorativi al di fuori della sede dell'amministrazione il salvataggio dei dati.

In caso di furto, danneggiamento o smarrimento del PC portatile l'utente è tenuto ad effettuare immediata segnalazione al proprio Responsabile e provvedere a immediata denuncia nelle forme di rito alle autorità di Pubblica Sicurezza

L'utilizzo di altre apparecchiature mobili (*palmari, telefoni cellulari e simili*) per la connessione ad internet, sia in modalità stand-alone sia per collegare i personal portatili, deve essere preventivamente autorizzata. La gestione di queste apparecchiature è a carico dell'utilizzatore. Su richiesta, il Servizio Sistemi Informativi fornirà i parametri necessari per la ricezione della posta elettronica su questi apparati (*indirizzo del mail server, etc*.).

6. Utilizzo delle stampanti e dei materiali di consumo
L'utilizzo delle stampanti e dei materiali di consumo in genere (*carta, inchiostro, toner, supporti magnetici, supporti digitali*) è riservato esclusivamente per lo svolgimento di compiti di natura strettamente istituzionale. Devono essere evitati in ogni modo sprechi dei suddetti materiali o utilizzi eccessivi.

7. Gestione delle password e degli account

Al fine di prevenire accessi non autorizzati ai sistemi informativi dell'amministrazione, ogni attività sulle risorse informatiche necessita di una preventiva autenticazione basata sulla combinazione di un identificativo utente (UserID) e una parola chiave (password). Per consentire l'accesso a reti, sistemi, dati o applicazioni è assegnato in modo univoco, ad ogni utente chiaramente identificato, uno User-ID al quale è associata una password. La responsabilità della segretezza della password è dell'assegnatario, il quale deve custodirla con cura senza rivelarla a nessuno, e deve astenersi dal trascriverla in qualsiasi forma. Qualora sussista il dubbio di violazione della segretezza, l'utente dovrà provvedere al cambiamento della password. Al primo accesso al sistema l'utente è obbligato a cambiare la password assegnata di default ed a porre in essere una gestione sicura della stessa nel rispetto dei seguenti requisiti:

- la password deve essere diversa dallo User-ID;
- non deve essere breve (minimo 8 caratteri);
- deve essere modificata dall'utente almeno ogni 90 giorni;
- è fatto divieto all'utente di utilizzare password banali, ovvie o facilmente memorizzabili; la password non deve essere costituita da predefinite sequenze alfanumeriche, né contenere riferimenti scontati o facilmente deducibili (nome del mese corrente, sequenze con numeri progressivi, etc.) o riferimenti a carattere personale (date, numeri di telefono, nomi di persona, etc.)

Si rende noto che nei casi in cui é indispensabile o indifferibile accedere ai dati trattati dall'utente ed agli strumenti informatici in dotazione allo stesso, sia per le esigenze organizzative e di servizio, sia per la sicurezza ed operatività dello stesso sistema informatico, il Servizio Sistemi Informativi del Comune potrà accedere agli strumenti elettronici personali, mediante l'intervento del personale appositamente incaricato ad operare, dietro richiesta del Responsabile al Trattamento dei dati. La stessa facoltà, sempre ai fini di garantire la salvaguardia e la sicurezza del sistema informatico e per ulteriori motivi tecnici e manutentivi, si applica anche in caso di assenza prolungata o impedimento dell'utente.

8. Profili di autorizzazione ed utilizzo della rete
I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati personali necessari per effettuare le operazioni di trattamento.

I profili vengono assegnati dai Responsabili del trattamento e devono indicare con esattezza i dati personali che l'incaricato è autorizzato a trattare.

Periodicamente, e comunque almeno annualmente, è verificata, da parte del Responsabile del trattamento, la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

9. Uso della posta elettronica

La casella di posta elettronica individuale viene assegnata d'ufficio agli Amministratori, ai dipendenti assunti a tempo indeterminato, a tempo determinato ed ai collaboratori che, per le funzioni svolte, sono dotati di personal computer.

L'Amministrazione comunale rende inoltre disponibili, oltre a quelli individuali, anche indirizzi di posta elettronica condivisi da più utenti. Tali indirizzi condivisi devono essere utilizzati esclusivamente per la ricezione di messaggi. INDIRIZZI CONDIVISI POSSONO ESSER RICHIESTI DAI RESPONSABILI I QUALI RISPONDERANNO DEL CORRETTO UTILIZZO DEGLI STESSI DA PARTE DEGLI UTILIZZATORI; E' CURA DEi RESPONSABILI INDIVIDUARE GLI INCARICATI AUTORIZZATI ALL'UTILIZZO.

La casella di posta elettronica assegnata è uno strumento di lavoro ed il suo utilizzo è consentito solo per finalità connesse allo svolgimento della propria attività lavorativa e per le comunicazioni di servizio di carattere sindacale. Le persone assegnatarie sono responsabili del corretto utilizzo della stessa.

E' fatto **divieto** di utilizzare la casella di posta elettronica per:

partecipazione a dibattiti, forum, o mailing-list non attinenti la propria attività o funzione svolta per l'Ente, salvo diversa ed esplicita autorizzazione del Dirigente del Servizio interessato.

Non è consentito l'invio di messaggi con allegati di dimensione superiori a **5 Mb** e con estensione uguali a **.bat .exe** ed in generale file di tipo eseguibile o di applicazione. Si precisa che il sistema di sicurezza e antivirus installato a protezione del server di posta elettronica del Comune di Ferrara non consente la ricezione e l'invio di messaggi di posta che contengono allegati con le caratteristiche sopra elencate. Eventuali esigenze particolari potranno essere segnalate alla struttura competente che individuerà la soluzione tecnica più appropriata.

In caso di assenza prolungata programmata del dipendente è raccomandata l'attivazione del sistema di risposta automatica ai messaggi di posta elettronica ricevuta indicando, nel messaggio di accompagnamento, le coordinate di un collega o della struttura di riferimento che può essere contattata e/o altre modalità utili di contatto della struttura cui il lavoratore è assegnato.

In caso di assenze dal lavoro**,** programmate o non programmate, e in presenza di improrogabili necessità legate all'attività lavorativa, qualora l'interessato non vi provveda direttamente accedendo alla propria casella di posta elettronica tramite l'apposito indirizzo web **https://mailer.comune.fe.it,** l'accesso alla posta elettronica può essere effettuato da un altro lavoratore delegato dall'interessato a verificare il contenuto e a inoltrare al Dirigente responsabile della struttura quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Di tale attività deve essere redatto apposito verbale e informato il dipendente interessato alla prima occasione utile.

In caso di cessazione del rapporto di lavoro, l'indirizzo di posta elettronica individuale dell'interessato viene mantenuto attivo per un periodo di tempo pari a quattro settimane salvo diversa indicazione del Dirigente di riferimento.

10. Uso della rete internet e relativi servizi
La rete internet è una risorsa messa a disposizione del personale come fonte di informazione per finalità di documentazione, ricerca e studio, utili per lo svolgimento delle mansioni assegnate. Quindi l'utilizzo di Internet deve essere limitato a scopi inerenti all'attività lavorativa.

L'Ente mette a disposizione dei dipendenti l'accesso ad Internet attraverso l'uso di un Proxy Server che, per ridurre il rischio di usi impropri della "navigazione web", consente di adottare opportune misure atte a prevenire controlli successivi.

In particolare l'Ente adotta una o più delle seguenti misure:

a. individuazione di categorie di siti considerati correlati o meno con la prestazione lavorativa;
b. configurazione di sistemi ed utilizzo di filtri che prevengano determinate operazioni reputate incoerenti con l'attività lavorativa (l'*upload,* l'accesso a determinati siti, il *download* di *file* o *software* aventi particolari caratteristiche dimensionali o di tipologia di dato);
c. utilizzo di file di log riferiti al traffico web per la produzione di report statistici con indicazione dei siti visualizzati ed individuazione delle aree di maggior traffico. L'attivita' statistica è fatta in forma anonima su dati aggregati che non consentono di risalire alle singole pagine navigate dall'utente.
d. conservazione dei dati strettamente limitata al perseguimento di finalità organizzative, produttive e di sicurezza.

II PC abilitato alla navigazione in Internet costituisce uno strumento necessario allo svolgimento della propria attività lavorativa. E' assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.

E' fatto divieto di utilizzare software **peer to peer** (P2P) per lo scarico di qualunque tipo di file (*esempio Emule*) ed è, inoltre, vietata la partecipazione a forum non professionali, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi.

11. Protezione antivirus
Al fine di proteggere i dati dal rischio di accesso abusivo e dall'azione dannosa di programmi (ad esempio v*irus),* l'Ente predispone a livello centralizzato, adeguati strumenti elettronici nonché il loro aggiornamento secondo le modalità previste dalla legge.

Il personale è tenuto a segnalare ogni malfunzionamento degli strumenti programmi antivirus, ed affini e per nessun motivo è autorizzato a disattivarli. Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo. E' tenuto, inoltre, a controllare la presenza e il regolare funzionamento del software antivirus aziendale.

Nel caso che il software antivirus rilevi la presenza di un virus che non è riuscito a ripulire, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer e segnalare l'accaduto al personale incaricato del SSI.

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 non eliminabile dal software, non dovrà essere utilizzato.

12. Mancata osservanza del Disciplinare

L'utente delle risorse informatiche del Comune di Ferrara che abbia violato il presente Disciplinare o la normativa ivi richiamata, potrà essere sottoposto ad azione disciplinare in conformità a quanto stabilito dai contratti collettivi**.**

Inoltre, nel caso in cui l'utilizzo non corretto degli strumenti informatici sopra descritti e assegnati al dipendente dovesse arrecare danno al funzionamento del sistema informativo del Comune, ovvero pregiudizio all'immagine dell'Ente o fosse configurato come reato, il Comune di Ferrara, oltre all'avvio delle procedure per l'adozione delle misure disciplinari, si riserva di far valere nelle sedi più opportune ogni altro suo diritto.

Nei confronti, poi, dei collaboratori e del personale non dipendente dell'Amministrazione comunale autorizzato a prestare la propria attività lavorativa all'interno del Comune di Ferrara, in caso di violazioni del presente disciplinare, saranno applicabili misure quali la revoca delle assegnazione e/o autorizzazioni all'uso di dispostivi e della rete informatica aziendale, la sospensione/interruzione/risoluzione del rapporto contrattuale in corso, nonché, in presenza dei necessari presupposti, il ricorso alle azioni amministrative e/o giudiziarie, anche di tipo risarcitorio, necessarie ai fini della tutela dei diritti e degli interessi dell'Amministrazione.

13. Controlli e verifiche

L'Amministrazione Comunale si riserva la facoltà di effettuare rilevazioni, anche saltuarie e occasionali, sull'osservanza delle sopra riportate disposizioni, nel rispetto della normativa vigente e dei **principi di proporzionalità** cioè nella pertinenza e non eccedenza delle attività di controllo e di **correttezza** per cui devono essere rese note al lavoratore in che misura e con quali modalità vengono effettuati i controlli atti a raccogliere dati personali. Sono esclusi controlli prolungati, costanti e indiscriminati.

In particolare, con riferimento alla disposizione di cui sopra, si precisa quanto segue:

per ridurre il rischio di usi impropri della **navigazione in Internet**, l'Amministrazione adotta accorgimenti tecnici e gestionali idonei ad impedire l'accesso ai siti Internet con contenuti in contrasto con la legislazione vigente, o che non abbiano attinenza con l'attività lavorativa quali:

- l'individuazione di categorie di siti considerati correlati o meno con la prestazione lavorativa;
- la configurazione di sistemi o utilizzo di filtri che prevengano determinate operazioni reputate pericolose o non inerenti con l'attività lavorativa.

L'attività di controllo è effettuata in forma graduata. In via preliminare saranno eseguiti controlli su dati aggregati riferiti all'intera struttura di rete o a sue aree omogenee a cui farà seguito, in caso di accertamento di irregolarità, un avviso al gruppo di utenti potenzialmente coinvolti che sono state riscontrate attività non conformi al presente Disciplinare, nonché l'invito al rispetto delle disposizioni impartite. Il Servizio Sistemi Informativi, in ogni caso, valuterà i possibili interventi

tecnici per prevenire il ripetersi delle anomalie e delle irregolarità riscontrate, proponendone l'adozione al Direttore Generale.

Nel caso in cui le irregolarità dovessero, comunque, ripetersi e nel caso in cui possa risultare compromessa l'operatività e la sicurezza della rete, su disposizione del Direttore Generale si procederà a cura del Servizio Sistemi Informativi all'individuazione delle postazione di lavoro interessate e alla eventuale sospensione dell'abilitazione di accesso alla rete internet. Il Servizio Sistemi Informativi provvederà, inoltre, a segnalare il comportamento anomalo al Dirigente della struttura di appartenenza del dipendente, per l'attivazione del procedimento disciplinare nelle forme e con le modalità previste dal C.C.N.L.

Per quanto riguarda **l'uso della posta elettronica**, tutti i messaggi inviati o ricevuti tramite il sistema di posta elettronica di proprietà del Comune di Ferrara possono essere sottoposti a verifica nelle forme previste dalla legge e nei limiti e con le modalità di seguito indicate.

In particolare, tutti i messaggi di posta elettronica ricevuti o inviati possono essere oggetto di rilevazione ai soli fini statistici e/o gestionali (ad es. per rilevare anomalie o per manutenzione).

Tuttavia, al fine di verificare l'osservanza alle presenti disposizioni, ove sussistano fondati dubbi di comportamenti non corretti o che mettono a rischio la funzionalità del sistema informativo dell'Ente, potrà essere autorizzato dal Direttore Generale il controllo da parte del Servizio Sistemi Informativi sui messaggi inviati o ricevuti dagli utenti.

Qualora sia accertata l'inosservanza alle presenti disposizioni, all'utente può essere sospeso o revocato l'account di posta elettronica. Il Servizio Sistemi Informativi provvederà, inoltre, a segnalare il comportamento al Dirigente della struttura di appartenenza del dipendente per l'attivazione del procedimento disciplinare nelle forme e con le modalità previste dal C.C.N.L.

In assenza di particolari esigenze tecniche o di sicurezza, la conservazione dei dati relativi all'uso degli strumenti elettronici è temporanea. I sistemi informatici utilizzati sono programmati e configurati in modo da cancellare periodicamente ed automaticamente attraverso procedure di sovraregistrazione i file di log relativi agli accessi, ad Internet, alla posta elettronica. Un eventuale prolungamento dei tempi di conservazione potrà aver luogo solo in relazione all'indispensabilità dell'informazione rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria o all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta di legge o dell'autorità giudiziaria.

_____

Il presente disciplinare, è stato, prima della sua diffusione tra tutti gli utilizzatori di strumenti informatici e telematici messi a disposizione dall'Amministrazione comunale, oggetto, ai sensi dell'art. 4, comma 2, della legge n.300/1970, di previo accordo con le rappresentanze dei lavoratori e di specifica preventiva informazione nei confronti dei lavoratori. Esso viene diffuso tra i dipendenti del Comune di Ferrara e adeguatamente pubblicizzato, oltre che nel sito web (internet e intranet) del Comune, a tutti gli utenti che facciano utilizzo di risorse strumentali informatiche dell'Ente.

I Responsabili dei Settori/Servizi/Unità Organizzative sono tenuti a vigilare affinché le presenti disposizioni siano comunicate a tutti gli utilizzatori delle risorse informatiche dell'Ente.

Inoltre, il dipendente deve attenersi, nell'utilizzo e nella gestione delle risorse strumentali informatiche comunali, ai principi e ai doveri contenuti nel "*Codice di comportamento dei dipendenti delle pubbliche amministrazioni*" di cui al Decreto Ministero Funzione Pubblica del 28/11/2000.

I documenti sopra richiamati (Deliberazione del Garante Privacy n.13/2007, D.M. della Funzione Pubblica del 28/11/2000 e Direttiva n.02/09 del Dipartimento della Funzione Pubblica) possono essere reperiti ai seguenti indirizzi internet:
http://www.garanteprivacy.it/garante/doc.jsp?ID=1387522
http://bancadati.digita-lex.it/public/files/pdf/0158_6-Direttiva_n2_09.pdf-

ALLEGATO A

GLOSSARIO DEI TERMINI TECNICI E INFORMATICI

Account	Iscrizione registrata su un server e che, tramite l'inserimento di una user id e di una password, consente l'accesso alla rete e/o ai servizi. Ad esempio, un account ci permette di entrare in Internet, un altro account ci serve per ricevere e spedire posta elettronica. Un account ci consente di accedere alle risorse di una rete locale, come server, file server, stampanti. Altri account servono per accedere a server e servizi vari.
Antivirus	Tipo di software che cerca e distrugge gli eventuali virus e cerca di rimediare ai danni che hanno compiuto.
Backup	Termine, che significa copia di sicurezza, indica l'operazione di duplicare su differenti supporti di memoria le informazioni (dati o programmi) presenti sui dischi di una stazione di lavoro o di un server. Normalmente viene svolta con una periodicità stabilita.
Chat	(letteralmente, "chiacchierata") è un servizio informatico che permette attraverso internet, di attivare e gestire un dialogo in tempo reale fra due o più utenti utilizzando principalmente messaggi testuali.
Database	(Base di Dati). Qualsiasi aggregato di dati organizzato in campo (colonne) e record (righe).
Dati giudiziari	I dati giudiziari sono quei dati personali in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti. Inoltre possono essere quei dati personali indicanti la qualità di imputato o di indagato.
Dati personali	(art. 4 c. 1 lett b) del D.lgs. 196/03) identificano le informazioni relative alla persona fisica, giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altro dato, ivi compreso un numero di riconoscimento personale.

Dati sensibili

secondo il Codice sulla protezione dei dati personali (d.lgs. 196/2003), art.4, sono considerati dati sensibili, e dunque la loro raccolta e trattamento sono soggetti sia al consenso dell'interessato sia all'autorizzazione preventiva del Garante per la protezione dei dati personali (art. 26), i dati personali, idonei a rivelare:

- l'origine razziale ed etnica,
- le convinzioni religiose, filosofiche o di altro genere,
- le opinioni politiche,
- l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale,
- lo stato di salute e la vita sessuale

Download

Registrare sul proprio disco rigido un file richiamandolo, tramite modem o rete, da un computer, da un server o da un host (tramite Internet, rete locale o geografica).

E-mail

Electronic mail, posta elettronica. Scambio di messaggi e di file attraverso una rete locale o Internet. Avviene in tempo reale ed è indipendente dalla posizione fisica dei computer mittente e destinatario. I messaggi e file vengono conservati da un server che provvede ad inoltrarli al destinatario quando questo si collega.

Firewall

Insieme di software/hardware usato per filtrare i dati in scambio fra reti diverse, al fine di proteggere un server da attacchi pervenuti via rete locale o via Internet. Consente il passaggio solamente di determinati tipi di dati, da determinati terminali e determinati utenti.

Hardware

Letteralmente ferramenta, in informatica si intende l'insieme dei componenti (CPU, Hard Disk ecc.) che costituiscono un computer.

ID utente:

Codice identificativo personale per l'accesso ai sistemi informatici. Normalmente è formato dall'iniziale del nome.cognome.

Internet

La madre di tutte le reti di computer. E' l'insieme mondiale delle reti di computer interconnesse.

Intranet	Rete locale che, pur non essendo necessariamente accessibile dall'esterno, fa uso di tecnologie Internet.
Guestbook	(libro degli ospiti) è un'utilità interattiva che permette ai visitatori di un sito web di poter lasciare traccia delle navigazioni.
Log	Termine, che significa giornale di bordo o semplicemente giornale, viene utilizzato nell'informatica per indicare la registrazione cronologica delle operazioni man mano che vengono eseguite ed il file su cui tali registrazioni sono memorizzate.
Password	(in italiano: "parola chiave", "parola d'ordine", o anche "parola d'accesso") è una sequenza di caratteri utilizzata per accedere ad una risorsa informatica.
Principio di necessità	è un principio generale dell'ordinamento che presiede all'adozione di tutte le misure straordinarie da parte delle Autorità.
Software freeware:	Programmi software distribuiti in modo gratuito.
Software peer-to-peer:	Programmi utilizzati per la condivisione e lo scambio di files fra elaboratori. Questi programmi vengono utilizzati principalmente per scambiarsi file di tipo mp3, (file musicali) e DivX (contenenti film) spesso in violazione dei diritti d'autore.
Stand-alone:	Si riferisce ad un'apparecchiatura capace di funzionare da sola, indipendentemente dalla presenza di altre apparecchiature con cui potrebbe comunque interagire.
User Id	Nome utente
Utente (User)	Chiunque utilizzi un elaboratore collegato alla rete, sia che il collegamento avvenga in rete locale sia che si tratti di un accesso remoto.
Unità di rete	Spazio disco condiviso che risiede fisicamente su altro computer o server
Virus	Programma creato per diffondersi da computer a computer, spesso danneggiando i dati e gli altri programmi.