COMUNE DI MARSCIANO
(PROVINCIA DI PERUGIA)

REGOLAMENTO SULL'UTILIZZO DEGLI STRUMENTI INFORMATICI CON RIGUARDO ALLA DISCIPLINA DELLA TUTELA DEI DATI PERSONALI

(Il presente regolamento è stato redatto tenendo conto delle linee guida del Garante della Privacy emanate con delibera n. 13 del 1° marzo 2007, del D.lgs 196/2003, della normativa vigente in tema di tutela del diritto d'autore e criminalità informatica e della legge 300/1990 riguardante lo statuto dei lavoratori).

INDICE

PREMESSA

Negli ultimi anni l'utilizzo di risorse informatiche (computer, periferiche, software, internet, interconnessione con altri soggetti) da parte del comune è notevolmente aumentato in quantità e complessità. Tutto ciò ha avuto importanti ricadute in termini di sicurezza esponendo l'ente nel suo complesso 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).

E' necessario quindi stabilire una serie di regole di comportamento che, nel rispetto della normativa vigente in tema di trattamenti di dati personali e relative misure minime di sicurezza, garantiscano:

- l'efficienza ed il corretto utilizzo delle risorse informatiche;
- la riservatezza delle informazioni e dei dati;
- il rispetto delle leggi in materia di risorse in informatiche;

Il presente regolamento ha, inoltre, lo scopo di informare gli interessati sulle finalità del controllo e sulle specifiche tecnologie adottate per effettuarlo.

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.

Capo I
-
DISPOSIZIONI GENERALI

Art. 1
Oggetto del regolamento

1. Il presente regolamento disciplina le modalità di accesso e l'utilizzo degli strumenti informatici e il conseguente trattamento di dati personali nel rispetto di quanto disposto dal Decreto Legislativo 30 giugno 2003, n. 196 e dal provvedimento del Garante per la protezione dei dati personali del 1 marzo 2007.
2. L'Amministrazione promuove ogni opportuna misura, organizzativa e tecnologica, volta a prevenire il rischio di utilizzi impropri delle strumentazioni e delle banche dati di proprietà del Comune di Marsciano.

Art. 2
Applicabilità

1. Le disposizioni del presente disciplinare sono applicabili a tutti gli **incaricati al trattamento** dei dati personali del Comune di Marsciano, a prescindere dal rapporto contrattuale che li lega all'Ente, e **a tutti coloro che utilizzano la strumentazione del Comune a qualsiasi titolo** ivi compresi programmi software, internet e/o caselle di posta elettronica.

Art. 3
Definizioni

1. Ai fini delle disposizioni contenute nel presente regolamento,
a) per **"utente"** deve intendersi ogni dipendente e collaboratore (collaboratore a progetto, in stage, agente, ecc.) che utilizza la strumentazione del Comune a qualsiasi titolo. Tale figura potrà anche venir indicata quale "incaricato del trattamento";
b) per **Sistema Informatico** – per brevità **S.I.** - del Comune di Marsciano deve intendersi "l'insieme coordinato dell'infrastruttura di rete telematica e degli apparati, elaboratori, software, archivi dati e/o risorse informative a qualsiasi titolo archiviate in modo digitale, in dotazione ed uso all'Amministrazione Comunale":
2. Per quanto attiene a tutte le altre definizioni presenti nel presente disciplinare, si fa riferimento a quanto disposto dall'Art. 4 del Decreto Legislativo 30 giugno 2003, n. 196, di seguito denominato "codice della privacy".

Art. 4
Principi Generali

1. Il Comune di Marsciano promuove l'utilizzo delle 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 e programmi cui ha accesso e dei dati trattati a fini istituzionali. E' 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. Sono vietati comportamenti che possono creare un danno, anche d'immagine, all'Ente.

Art. 5
Incaricati

1. Sono nominati incaricati del trattamento tutti i dipendenti a tempo indeterminato, a tempo determinato, i collaboratori ed ogni altra persona fisica che a qualunque titolo tratta dati personali per conto del Comune di Marsciano ed è ad esso legato da un rapporto contrattuale.
2. Gli incaricati possono trattare solo i dati personali necessari allo svolgimento della funzione alla quale sono stati assegnati dal proprio responsabile di riferimento.
3. Nel trattare i dati personali di cui al comma 2, gli incaricati dovranno attenersi, oltre a quanto disposto dalla legislazione vigente, anche alle disposizioni del presente disciplinare e a quelle ulteriori eventualmente impartite dal proprio responsabile di riferimento.
4. Gli incaricati dovranno vigilare, per quanto di loro competenza, sulla corretta applicazione e funzionamento delle misure di sicurezza a tutela della riservatezza dei dati personali trattati, ed informare immediatamente il responsabile del trattamento di riferimento in caso di malfunzionamento delle misure stesse.
5. Ai fini del presente regolamento **sono equiparati agli incaricati anche tutti gli amministratori** (sindaco, assessori, consiglieri comunali) nonché i **componenti delle commissioni** che trattano dati personali per lo svolgimento delle loro funzioni istituzionali.

Art. 6
Acquisto di strumenti informatici hardware e software

1. Per proteggere l'integrità del S.I. e al fine di garantire la sicurezza, l'inalterabilità e la disponibilità delle banche dati, tutto l'hardware ed il software acquistato deve essere conforme alle disposizioni contenute nell'allegato B del D.lgs 196/2003.
2. Il responsabile del S.I. (Sistema Informatico) e gli Amministratori di Sistema non sono responsabili degli strumenti informatici, indipendentemente dalle azioni di cui al successivo articolo 11, che provengano da acquisti non eseguiti con la loro approvazione

Art. 7
Competenze e responsabilità

1. Le competenze e le responsabilità del personale dell'Amministrazione Comunale ed in generale degli utenti del S.I. per ciò che concerne l'utilizzo della strumentazione, sono definite nei commi seguenti.
2. Il **Responsabile del Servizio Informatico** è tenuto a:
a) informare il personale sulle disposizioni in merito all'uso consentito delle risorse del sistema informativo dell'Ente attraverso la consegna e/o la pubblicazione del presente regolamento;
b) implementare le policy di sicurezza sul S.I.;
c) elaborare delle regole per un utilizzo ragionevolmente sicuro del sistema informativo.

3. I **Responsabili dei vari Servizi** sono tenuti a:
a) informare il personale sulle disposizioni in merito all'uso consentito delle risorse del sistema informativo dell'Ente;
b) assicurare che il personale a loro assegnato si uniformi alle regole ed alle procedure descritte nel presente Regolamento;
c) comunicare tempestivamente al Servizio Informatico comunale l'ingresso e/o la cessazione dal servizio di ogni dipendente o collaboratore che abbia necessità di operare sulle stazioni di lavoro, in modo da provvedere alla creazione/ cessazione delle relative credenziali di accesso al S.I.

d) adempiere a tutti gli obblighi inerenti la Responsabilità loro affidata in materia di trattamento di dati personali gestiti dall'Amministrazione Comunale, come previsto dal Documento Programmatico sulla Sicurezza.

4. Gli **amministratori di sistema e i tecnici informatici**, in generale, sono incaricati di:

a) monitorare i sistemi per individuare un eventuale uso scorretto degli stessi, nel rispetto della privacy degli utenti;
b) segnalare prontamente al responsabile del servizio informatico ogni eventuale attività non autorizzata sui sistemi.

5. Il **responsabile della sicurezza informatica, gli amministratori di sistema e i tecnici informatici sono autorizzati** 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 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, può avvenire anche senza aver preventivamente informato l'utente assegnatario della postazione.

6. L'utente del SI è responsabile per ciò che concerne:

a) il rispetto delle regole dell'Amministrazione per l'uso consentito del S.I.;
b) la segnalazione senza ritardo di ogni eventuale attività non autorizzata di cui sia venuto a conoscenza per motivi di ufficio;
c) ogni uso che venga fatto delle credenziali (account, passwords, user) e della strumentazione assegnategli.

Capo II
-
RAPPORTI CON IL PUBBLICO

Art. 8
Rapporti di front-office

1. Rispetto della distanza di sicurezza: per quanto riguarda gli operatori di sportello (cosidetto front office) deve essere prestata attenzione al rispetto dello spazio di cortesia e, se del caso, invitare gli utenti a sostare dietro la linea tracciata sul pavimento ovvero dietro le barriere delimitanti lo spazio di riservatezza.

2. Identificazione dell'interessato:in alcuni casi può essere necessario dover identificare il soggetto interessato per esigenze di garanzia e/o di correttezza del dato da raccogliere (si pensi a soggetti stranieri ovvero a dati identificativi che possono generare dubbi sulla correttezza della registrazione) ovvero con riferimento alla natura della prestazione richiesta può essere necessario richiedere ed ottenere un documento di identità o di riconoscimento ove si abbia un dubbio sulle modalità di scrittura del nome e cognome dell'interessato o si voglia avere garanzia dell'effettiva identità del soggetto interessato.

3. Controllo dell'esattezza del dato: fare attenzione alla digitazione ed all'inserimento dei dati identificativi dell'interessato, al fine di evitare errori di battitura, che potrebbero creare problemi nella gestione dell'anagrafica e nel proseguo del processo.

4. Obbligo di riservatezza e segretezza: l'incaricato del trattamento deve mantenere l'assoluta segretezza sulle informazioni di cui venga a conoscenza nel corso delle operazioni del trattamento e deve evitare qualunque diffusione delle informazioni stesse. Si ricorda che l'eventuale violazione dell'obbligo ivi considerato può comportare l'applicazione di sanzioni di natura disciplinare ed una responsabilità civile e penale, secondo quanto previsto dal codice della privacy.

Art. 9
Cautele da seguire per la corretta comunicazione dei dati a soggetti terzi

1. Controllo dell'identità del richiedente: nel caso di richieste di comunicazione di dati (presentate per telefono, per fax o per e-mail) occorre verificare l'identità del soggetto richiedente, ad esempio formulando una serie di quesiti a mezzo intervista guidata. In altri casi, a tutela della riservatezza del dato con riferimento allo specifico procedimento, il Responsabile di settore attribuisce all'interessato un codice personale identificativo, da comunicare al personale interno dell'ente per ogni comunicazione impersonale (ad esempio a mezzo telefonico).
2. Verifica dell'esattezza dei dati comunicati: nell'accogliere una richiesta di comunicazione di dati personali da parte dell'interessato ovvero di un terzo a ciò delegato, occorre fare attenzione all'esattezza del dato che viene comunicato, in particolare quando la richiesta viene soddisfatta telefonicamente o attraverso trascrizione da parte dell'operatore, di quanto visualizzato sul monitor.

Art. 10
Presenza di ospiti o di personale di servizio

1. L'incaricato deve fare attendere gli ospiti in luoghi in cui non siano presenti informazioni riservate o dati personali.
2. Nel caso in cui l'incaricato debba allontanarsi dalla scrivania in presenza di ospiti, egli deve riporre i documenti e attivare uno dei sistemi di protezione previsti dal successivo Art. 24.
3. L'incaricato non deve rivelare o fare digitare le password al personale di assistenza tecnica.
4. L'incaricato non deve rivelare le password in alcun modo, in quanto nessuno è autorizzato a chiederle.
5. L'incaricato deve segnalare qualsiasi anomalia o stranezza al proprio responsabile.

Capo III
-
ISTRUZIONI PER L'USO DEGLI STRUMENTI DEL TRATTAMENTO

Art. 11
Regole di utilizzo della strumentazione a carattere generale

1. La strumentazione di proprietà dell'Amministrazione Comunale viene data in uso agli utenti per lo svolgimento dei compiti assegnati e non può essere utilizzata per altri scopi.
Può essere tollerato un uso personale di questi strumenti solo in caso di comprovata necessità ed urgenza.
2. La strumentazione utilizzata deve essere custodita con cura evitando ogni possibile forma di danneggiamento.
3. Ogni utilizzo non correlato con l'attività lavorativa, oltre a configurarsi come attività non lecita, può contribuire ad innescare disservizi, costi di manutenzione e minacce alla sicurezza dell'intera rete. L'utente sarà sempre ritenuto responsabile per eventuali danni provocati dall'uso delle attrezzature per scopi diversi da quelli relativi ai compiti assegnati.
4. La strumentazione è oggetto di apposito censimento, pertanto non può disporsi l'assegnazione della stessa ad altro utente né lo spostamento della stessa in altri locali senza averlo prima comunicato all'ufficio Patrimonio e – per quanto riguarda computer e stampanti – anche all'ufficio Informatico.

In assenza di apposita comunicazione, l'utente a cui la strumentazione risulta assegnata sarà ritenuto direttamente responsabile dei danni o dello smarrimento della stessa.

Art. 12
Utilizzo dei personal computer

1. Sui personal computer di proprietà del Comune di Marsciano è consentito il solo utilizzo connesso allo svolgimento delle attività istituzionali dell'ente.
   L'accesso al personal computer può avvenire solo attraverso specifiche **credenziali di autenticazione** come meglio descritto al successivo Art. 21 del presente Regolamento
2. Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal personale del Servizio Informatico 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 l'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.
3. Non è consentito (se non preventivamente autorizzati dal personale del Servizio informatico):
   a) modificare le configurazioni relative all'accesso alla rete (ad esempio indirizzo IP);
   b) attivare l'accesso dall'esterno ad un sistema di calcolo se non preventivamente comunicato al responsabile di riferimento o all'amministratore di sistema;
   c) installare modem per l'accesso da/all'esterno;
   d) connettere dispositivi esterni personali (chiavi USB, hard disk, stampanti, ecc.);
   e) copiare su dispositivi esterni personali dati la cui titolarità è del Comune di Marsciano;
   f) installare autonomamente programmi o applicativi;
4. Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici, 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, pertanto in caso di assenza temporanea dalla propria postazione di lavoro è opportuno bloccare il computer in modo che venga riattivato solo con l'inserimento delle credenziali di autenticazione.

Art. 13
Utilizzo dei computer portatili

1. L'utente è responsabile del PC portatile assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
2. Ai PC portatili si applicano le regole di utilizzo previste dal precedente art.12 con particolare attenzione alla rimozione di eventuali file elaborati prima della riconsegna;
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 sia dello strumento che dei dati ivi conservati.
4. La persona che utilizza il portatile sarà ritenuto responsabile di eventuali danni e/o furti dei dati dovuti ad un uso improprio
5. Tali disposizioni si applicano anche nei confronti di incaricati esterni che utilizzano propri strumenti di lavoro per gestire banche dati di proprietà del Comune di Marsciano.

Art. 14
Utilizzo e conservazione dei supporti rimovibili

1. Tutti i supporti magnetici rimovibili (dischetti, CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati sensibili nonché dati personali o banche dati di proprietà 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.

2. Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale del Servizio Informatico nel caso in cui siano rilevati virus ed adottando quanto previsto dal successivo Art. 23 del presente Regolamento relativo alle procedure di protezione antivirus.
3. I supporti magnetici contenenti dati sensibili devono essere adeguatamente custoditi dagli utenti in armadi chiusi e/o protetti con sistemi di crittazione.
4. L'utente è responsabile della custodia dei supporti e dei dati aziendali in essi contenuti.

Art. 15
Riutilizzo e distruzione dei supporti di memorizzazione

1. I supporti di memorizzazione sia fissi (hard disk) che rimovibili (floppy-disk, cd, dvd, chiavi USB, hard disk esterni, ecc.) possono essere riutilizzati da terzi solo se i dati precedentemente memorizzati non siano più visionabili da parte dei soggetti che procedano al riutilizzo del supporto medesimo.
2.. Nel caso in cui i supporti di memorizzazione contengano dati sensibili e/o giudiziari il riutilizzo è possibile solo dopo la cancellazione sicura con sistemi software a passaggio multiplo (degauss).
3. Qualora sia necessario dismettere un supporto di memorizzazione, si dovrà procedere a rendere inintelligibile il contenuto, attraverso la distruzione dello stesso, oppure attraverso l'uso di sistemi di degauss.

Art. 14
Utilizzo degli scanner

1. I soggetti che provvedano all'acquisizione in formato digitale della documentazione cartacea devono verificare che l'operazione avvenga correttamente e che il contenuto del documento oggetto di scansione sia correttamente leggibile. Qualora vi siano errori di acquisizione ovvero si verifichino anomalie di processo, occorrerà procedere alla ripetizione delle operazioni.
2. E' severamente vietato l'uso di scanner di rete per l'acquisizione di dati sensibili e/o giudiziari nel caso in cui i documenti vengono posizionati su cartelle condivise da utenti che non hanno accesso a tali dati.
3. In ogni caso, l'incaricato che ha effettuato la scansione deve provvedere quanto prima a rimuovere l'informazione dalla cartella condivisa.

Art. 15
Utilizzo delle stampanti

1. Nella stampa di documenti è necessario – per motivi di economicità - privilegiare l'uso delle stampanti di rete e usare le stampanti locali solo in caso di effettiva bisogno.
2. E' necessario prestare attenzione affinché vengano lasciati documenti sulle stampanti di rete.

Art. 16
Utilizzo del Telefono

1. Nel caso di richieste di informazioni da parte di organi di amministrazioni pubbliche, o di autorità giudiziarie, può essere necessario, a seconda della natura dei dati richiesti, procedere nel seguente modo:
a) chiedere l'identità del chiamante e la motivazione della richiesta;
b) richiedere il numero di telefono da cui l'interlocutore sta effettuando la chiamata;
c) verificare che il numero di telefono dichiarato corrisponda effettivamente a quello del chiamante (ad esempio caserma dei carabinieri, servizi pubblici e di PS, …);

d) procedere immediatamente a richiamare la persona che ha richiesto le informazioni, con ciò accertandosi dell'identità dichiarata in precedenza.

Art. 17
Utilizzo del Fax

1. Nell'utilizzare questo strumento occorre prestare attenzione a:

a) digitare correttamente il numero di telefono, cui inviare la comunicazione;
b) controllare l'esattezza del numero digitato prima di inviare il documento;
c) verificare che non vi siano inceppamenti della carta ovvero che non siano presi più fogli contemporaneamente;
d) attendere la stampa del rapporto di trasmissione, verificando la corrispondenza tra il numero di pagine da inviare e quelle effettivamente inviate;
e) qualora siano trasmessi dati idonei a rivelare lo stato di salute, è necessario anticipare l'invio del fax chiamando il destinatario della comunicazione al fine di assicurarsi che il ricevimento avverrà nelle mani del medesimo, evitando che soggetti estranei o non autorizzati, possano conoscere il contenuto della documentazione inviata;
f) ove l'utente lo ritenga opportuno, lo stesso provvede a richiedere una telefonata che confermi da parte del destinatario la circostanza della corretta ricezione e leggibilità del contenuto del fax.

Art. 18
Distruzione delle copie cartacee

1. Coloro che sono preposti alla duplicazione di documentazione (con stampanti o fotocopiatrici o altre periferiche) ovvero alla sostituzione della documentazione cartacea con registrazione ottica devono procedere alla distruzione controllata dei supporti cartacei non più occorrenti ovvero che presentino una forma non corretta.

2. Occorre evitare di gettare la documentazione nel cestino della carta straccia senza aver previamente provveduto a rendere inintelligibile il contenuto. Qualora sia necessario distruggere i documenti contenenti dati personali, questi devono essere distrutti utilizzando gli appositi apparecchi "distruggi documenti" o, in assenza, devono essere sminuzzati in modo da non essere più ricomponibili.

Art. 19
Utilizzo dei materiali di consumo

1. L'utilizzo dei materiali di consumo (carta, inchiostro, toner, CD, DVD, chiavi USB, ecc.) è riservato esclusivamente alla preparazione di materiale inerente l'attività istituzionale dell'Ente. Devono essere evitati in ogni modo sprechi dei suddetti materiali o utilizzi eccessivi**.**

Art. 20
Strumenti Informatici NON di proprietà del Comune di Marsciano

1. Per il trattamento dei dati personali non è consentito l'utilizzo di strumenti informatici non di proprietà del Comune di Marsciano, salvo che per ragioni di comprovata necessità ed urgenza.
In questo caso occorre autorizzazione scritta del Responsabile del Trattamento dati.

2. L'utilizzo di strumenti non di proprietà del Comune di Marsciano è a totale responsabilità di chi ne fa uso, che ne risponde amministrativamente, civilmente e penalmente, secondo le norme applicabili.

3. Le attività di aggiornamento di antivirus e degli applicativi sono interamente a carico del proprietario.
4. L'Ente non è in alcun modo responsabile di eventuali danni o malfunzionamenti di tali strumentazioni.

Capo IV
-
ADOZIONE MISURE MINIME PER LA SICUREZZA DEI DATI

Art. 21
Credenziali di autenticazione

1. L'accesso al dominio e alle procedure informatiche che comportino il trattamento di dati personali 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 (user-id o username) associato ad una parola chiave riservata (password), oppure in un dispositivo di autenticazione (es. smart card) o in una caratteristica biometrica.
3. Gli incaricati sono responsabili della custodia e dell'utilizzo delle proprie credenziali di autenticazione e devono utilizzarle e gestirle attenendosi alle seguenti istruzioni:
a) la parola chiave, assegnata a ciascun incaricato, è composta da un minimo di otto caratteri o comunque dal numero massimo di caratteri consentito dal sistema;
b) la parola chiave assegnata deve essere prontamente sostituita dall'incaricato al primo utilizzo e deve essere modificata con cadenza almeno semestrale (trimestrale se l'utente tratta dati sensibili e/o giudiziari);
c) la password non deve contenere riferimenti agevolmente riconducibili all'incaricato e deve essere generata preferibilmente senza un significato compiuto;
d) l'incaricato, nello scegliere la propria password, deve utilizzare anche caratteri speciali, numeri, lettere maiuscole e minuscole. L'incaricato non deve scegliere come password parole presenti in un dizionario, sia della lingua italiana che di lingue straniere, ne utilizzare parole ottenute come combinazione di tasti vicini sulla tastiera o sequenze di caratteri (ad esempio qwerty, asdfgh, 123321, aabbcc, ecc.);
e) la parola chiave deve essere custodita con la massima attenzione e segretezza e non deve essere divulgata o comunicata a terzi;
f) la parola chiave non deve essere scritta su nessun tipo di supporto (cartaceo, elettronico, ecc.);
g) l'incaricato è responsabile di ogni utilizzo indebito o non consentito delle credenziali di autenticazione di cui sia titolare;
h) nel caso in cui altri utenti debbano poter accedere ai dati protetti dalle credenziali di un utente assente o impedito, è necessario richiedere l'autorizzazione al Responsabile del trattamento dietro richiesta scritta motivata. Il Servizio Informatico provvederà a resettare la parola chiave dell'utente assente o impedito il quale, al suo ritorno, dovrà procedere nuovamente al cambio della stessa; la procedura è spiegata nel dettaglio più avanti;
i) le credenziali di autenticazione individuali per l'accesso alle applicazioni non devono mai essere condivise tra più utenti (anche se incaricati del trattamento). Qualora un utente dovesse avere la necessità di trattare dati o usare le procedure, il responsabile di riferimento potrà richiedere formalmente le relative credenziali di autenticazione dotate dei privilegi necessari all'accesso ai dati o ai servizi richiesti;
l) se l'incaricato ha il sospetto di una perdita di qualità delle proprie credenziali (ad es. perché crede che queste siano conosciute da altri) è tenuto immediatamente a procedere al cambio della parola chiave.

m) nel caso l'incaricato dimentichi la propria password, dovrà chiedere formalmente al Servizio Informatico l'assegnazione di una nuova parola chiave da gestire come indicato al precedente Punto 3 lettera b).

4. Il responsabile del Sistema Informatico e gli Amministratori di sistema non sono responsabili in merito alla politica di gestione degli accessi a procedure che non siano da essi gestite/assegnate (es. procedure acquistate senza approvazione tecnica, software esterni all'ente, ecc).

Art. 22
Back-up

1. Salvo che **non sia previsto un sistema di salvataggio di dati personali automatico ovvero centralizzato**, occorre procedere con cadenza almeno settimanale alla effettuazione di copie di sicurezza dei dati personali oggetto di trattamento, utilizzando DVD o eventuali altri apparati che siano messi a disposizione dell'incaricato e consegnare i supporti contenenti le copie di salvataggio al soggetto nominato e incaricato della conservazione, ovvero riporre le copie in un contenitore al quale possano accedere solamente soggetti autorizzati.

2. Viene ribadito quanto prescritto dall'Allegato B al D.Lgs. n. 196/2003 (Disciplinare tecnico in materia di misure minime di sicurezza).

3. Le **Banche dati non censite** (anche se salvate su server sottoposti a politiche di backup) o memorizzate su unita locali (es disco C:) ovvero in generale create dai singoli utenti, **non** sono soggette a salvataggio da parte del personale informatico incaricato. **La responsabilità del salvataggio dei dati è pertanto a carico del singolo utente.**

Art. 23
Antivirus

1. Il Comune di Marsciano si è dotato di un sistema centralizzato e automatizzato di protezione antivirus. E' fatto divieto sospendere, cancellare o alterare in alcun modo il sistema antivirus anche se il suo funzionamento possa comportare un calo nelle prestazioni delle postazioni di lavoro; ogni danno conseguente alla manomissione del sistema antivirus sarà addebitato al manomissore.

2. E' compito degli incaricati verificare il corretto funzionamento ed aggiornamento del software antivirus, avvisando il Servizio Informatico qualora riscontrassero anomalie.

3. Laddove non siano adottati sistemi automatici di aggiornamento dei sistemi di protezione da virus, gli incaricati del trattamento devono procedere all'effettuazione delle operazioni di aggiornamento dei programmi ivi considerati, almeno con cadenza settimanale o quando sia segnalata dal sistema tale esigenza, secondo le istruzioni visualizzate sullo schermo; una volta scaricato l'aggiornamento occorre procedere alla scansione dell'intero sistema per verificare la presenza sull'elaboratore in dotazione di virus.

Art. 24
Protezione degli strumenti di lavoro

1. In caso di assenza, anche momentanea, dalla propria postazione di lavoro, devono essere adottate misure atte a escludere che soggetti non autorizzati possano acquisire la conoscenza di informazioni o accedere alle banche dati. A tal proposito è necessario adottare un sistema di oscuramento (cd. screen-saver) dotato di password, ovvero di uscire dal programma che si sta utilizzando, ovvero, in alternativa, occorrerà porre la macchina in posizione di stand-by o spegnere l'elaboratore che si sta utilizzando.

2. Coloro che utilizzano computer portatili devono adottare tutte le misure necessarie atte a non subire furti di dati ed in particolare è necessario non lasciare mai incustoditi tali computer ed evitare la memorizzazione in locale di dati sensibili e/o personali. Qualora non sia possibile

salvare i dati personali sul server di rete ed il portatile venga utilizzato al di fuori dei locali comunali occorre procedere alla crittazione degli stessi.

Art. 25
Software installati

1. Sui PC devono essere installati esclusivamente software necessari all'attività lavorativa, dotati di licenze d'uso legali e forniti dalle strutture di appartenenza. Sono vietati i software scaricati da Internet o acquisiti autonomamente se non preventivamente autorizzati dal Servizio Informatico e/o dal Responsabile del Servizio/Ufficio. I software installati senza autorizzazione verranno rimossi senza alcun preavviso. Il fatto sarà formalmente segnalato al Responsabile competente per i provvedimenti disciplinari.

2. Sui PC devono essere installati, appena sono resi disponibili (e comunque almeno annualmente), tutti gli aggiornamenti software necessari a prevenirne vulnerabilità e correggerne i difetti.

3. Il Responsabile del Sistema Informatico non è responsabile dei software, indipendentemente dalle azioni di cui ai commi 1 e 2 del presente articolo, che provengano da acquisti non eseguiti con la sua approvazione.

Capo V
-
POSTA ELETTRONICA

Art. 26
Indirizzo di posta elettronica

1. Ogni utente può essere dotato di un indirizzo di posta elettronica istituzionale personale o di ufficio. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

2. La casella di posta elettronica è parte integrante dell'attività lavorativa e come tale deve essere conservata e archiviata al fine di successive attività, si suggerisce pertanto di evitare per qualsiasi ragione l'invio di e-mail prive di oggetto.

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

a) Trasmissione di dati sensibili, salvo i casi espressamente richiesti dalla normativa vigente in materia;
b) Trasmissione di dati confidenziali e personali di alcun genere, salvo i casi espressamente previsti dalla normativa vigente in materia di protezione dei dati personali;
c) Partecipazione a dibattiti, forum o mailing list non attinenti la propria attività o funzione svolta per l'Ente, salvo diversa ed esplicita autorizzazione;
d) la partecipazione a catena telematiche (o di Sant'Antonio).

4. E' vietata qualsiasi attività che può, in qualsiasi modo, recare danno all'immagine dell'Ente

5. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili soprattutto SPAM e eliminando gli allegati ingombranti.

6. In caso di assenza programmata (ad es. per ferie) l'utente dovrà attivare la funzionalità messe a disposizione del servizio di e-mail atte a garantire la continuità operativa dell'ufficio senza consegnare le proprie credenziali a terzi (quale l'inoltro della propria posta ad altra casella).

7. In caso di assenza non programmata (ad es. per malattia), qualora l'utente non possa attivare entro due giorni la funzionalità di cui al precedente punto 4 avvalendosi del servizio webmail – tale funzionalità potrà essere attivata a cura del servizio Informatico su richiesta del superiore gerarchico dell'utente.

In tal caso è necessario resettare la password.

7. Sarà comunque consentito al superiore gerarchico dell'utente o, comunque, a persona individuata dall'Ente, accedere alla casella di posta elettronica dell'utente per ogni ipotesi in cui si renda necessario.

8. Il personale del servizio informatico, 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 precedente punto 7.

9. Gli uffici che lo richiedano possono disporre di una casella di posta elettronica istituzionale "di ufficio". La casella di posta elettronica di ogni singolo ufficio può essere utilizzata secondo quanto stabilito dal responsabile e comunque nel rispetto del presente regolamento.

Art. 27
Riservatezza degli indirizzi di posta elettronica

1. E' assolutamente vietato comunicare in qualsiasi modo gli indirizzi di posta elettronica di altri utenti all'esterno del Comune di Marsciano o a servizi gestiti al di fuori della rete del Comune di Marsciano.

2. Qualora si debbano inviare e-mail a più utenti usare la "copia nascosta" o "Ccn".

3. Quanto disposto dai precedenti Punti 1 e 2 non si applica alle attività sindacali e/o strettamente istituzionali quali la diffusione di circolari.

Art. 28
Lettura degli allegati

1. E' fatto divieto aprire messaggi, sia manualmente sia in forma automatica, con allegati di cui non si conosce l'origine. Essi possono contenere virus in grado di danneggiare e/o cancellare i dati sul PC.

2. E' fatto divieto di aprire filmati e presentazioni non attinenti l'attività lavorativa per evitare situazioni di pericolo per i dati contenuti sul vostro PC.

Capo VI
-
INTERNET

Art. 29
Autorizzazione all'uso di internet

1. L'accesso ad Internet è consentito a tutti gli incaricati del Comune di Marsciano per lo svolgimento delle proprie attività istituzionali, mediante le attrezzature informatiche messe loro a disposizione.

2. L'utilizzo di internet deve essere limitato a scopi inerenti l'attività lavorativa.

3. Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa la navigazione in internet viene filtrata attraverso appositi sistemi installati in modo centralizzato secondo le modalità indicate nei successivi articoli 30 e31.

4. Solo gli utenti espressamente abilitati hanno accesso ad una navigazione con regole di filtraggio personali. L'abilitazione è concessa previa motivata richiesta scritta del responsabile di riferimento a cui appartiene l'incaricato.

Art. 30
Meccanismi di controllo automatizzati

1. Il sistema di filtraggio del traffico è basato sull'adozione di black list e/o white list adottate dal Servizio Informatico nel rispetto delle normative vigenti e previo accordo con gli Amministratori dell'ente e i responsabili di servizio/ ufficio.

2. Gli strumenti utilizzati, nel rispetto delle normative vigenti in materia di rapporto di lavoro e del Codice della Privacy, attuano un controllo preventivo sulle attività compiute durante la navigazione e impediscono in maniera automatizzata la maggior parte degli usi impropri della rete Internet. I filtri automatici, impedendo all'origine tutta una serie di attività ritenute dannose, evitano che sia effettuato un controllo sistematico della navigazione del singolo utente, a vantaggio della privacy.

3. Al fine di garantire l'attuazione di misure preventive sul controllo della navigazione, la selezione di siti cui non è possibile accedere (black list) può essere modificata con cadenza mensile su richiesta del Sindaco e/o dei responsabili sulla base dei report di tipo aggregato generati dal sistema di filtraggio.

3. 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 Marsciano, il Responsabile del Servizio Informatico o altro soggetto che ne ha facoltà può autorizzare l'Amministratore di Sistema ad individuarne le cause e l'origine.

Art. 31
Modalità di controllo della navigazione in internet

1. Sarà inoltre preferito, per quanto possibile, un controllo preliminare su dati aggregati, riferiti all'intera struttura lavorativa o a settori/uffici. Il primo controllo avverrà infatti effettuando verifiche di Settore, di Ufficio o di Gruppo di lavoro in modo da individuare il problema in maniera "impersonale"; il settore, ufficio o gruppo ritenuto responsabile del traffico anomalo sarà richiamato all'osservanza scrupolosa delle regole. Soltanto in seguito, e al ripetersi dell'anomalia, si procederà a controlli su base individuale.

2. Se quanto previsto al comma 1, non sarà sufficiente ad individuare l'origine e la causa, l'ente si riserva il diritto di effettuare controlli sull'uso degli strumenti elettronici evitando in ogni modo ogni forma di ingerenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata.

3. In ogni caso, i controlli saranno sempre limitati nel tempo, ed effettuati dopo preavviso all'interessato in maniera continua, per il tempo strettamente necessario alla individuazione della causa ed origine e mirati nei confronti del rispetto delle disposizioni di legge.

4. Le registrazioni del traffico effettuato saranno conservate per un periodo non inferiore a ventiquattro mesi, elevabile fino ad ulteriori ventiquattro mesi e in ogni caso, in conformità con la normativa vigente, ai fini di permettere un'indagine a posteriori di eventuali anomalie e problemi di sicurezza. I dati sul traffico conservati ai fini di indagini non saranno consultabili se non dalle forze dell'ordine o, previa autorizzazione motivata del responsabile di riferimento o in sua assenza dal funzionario responsabile del Sistema Informatico.

Art. 32
Comportamenti non tollerati

1. E' fatto divieto di utilizzare la navigazione in Internet per usi non istituzionali. In particolare non sono permesse le seguenti attività se non preventivamente autorizzate:

a) scaricare (download) qualunque genere di file o programma salvo non sia indispensabile per svolgere l'attività lavorativa a cui il dipendente è preposto;
b) caricare (upload) files di qualunque genere presso siti esterni alla rete del Comune di Marsciano salvo non sia indispensabile per svolgere l'attività lavorativa a cui il dipendente è preposto;
c) consultare e utilizzare posta elettronica esterna o diversa da quella istituzionale tramite portali internet (web mail) se non per tempi limitati e/o per ragioni lavorative;
d) partecipare a chat, blog o Forum esterni alla rete del Comune di Marsciano;
e) utilizzare protocolli di streaming che consentono ad esempio di ascoltare radio o vedere materiali video da siti diversi da quelli istituzionali;
f) l'utilizzo di programmi peer to peer;
g) registrazione a siti i cui contenuti non siano legati con l'attività istituzionale;

2. L'elenco sopra riportato non si intende come esaustivo e verrà pertanto impedito ogni altro tipo di utilizzo ritenuto dannoso per l'Ente.

3. Non è consentito collegare alla rete dell'ente, anche tramite collegamento WiFi, attrezzature di calcolo personali o comunque non di proprietà del Comune di Marsciano, se non preventivamente autorizzate dal responsabile di riferimento. In ogni caso il loro utilizzo dovrà avvenire in conformità al presente regolamento.

4. Non è inoltre consentito collegare alla rete dell'ente apparati di rete (Access Point WiFi, router, switch, …) se non preventivamente autorizzati dal Servizio Informatico. In ogni caso il loro utilizzo dovrà avvenire in conformità al presente regolamento.

Capo VII
-
USO DI STRUMENTAZIONE INFORMATICA PER CORSI E MANIFESTAZIONI IN GENERALE

Art. 33
Indicazioni a carattere generale

1. L'utilizzo di strumenti informatici per l'organizzazione di corsi o manifestazioni in generale può avvenire solo previa richiesta / prenotazione che deve essere formalizzata per iscritto all'ufficio incaricato della gestione.
Qualora la richiesta venga fatta per manifestazioni non organizzate direttamente dall'Ente è necessaria autorizzazione scritta da parte del Sindaco o della Giunta Comunale.

2. La strumentazione informatica concessa in uso per la realizzazione di corsi e/o di manifestazioni è sottoposta a tutte le disposizioni del presente regolamento. Pertanto al momento della consegna, chi prende in carico la strumentazione deve sottoscrivere apposito documento nel quale si assume la responsabilità della custodia dei beni consegnati sino alla loro restituzione ed in particolare prende visione delle seguenti disposizioni:
- La strumentazione viene data in uso solo per lo svolgimento del corso e/o della manifestazione oggetto della richiesta e non può essere utilizzata per altri scopi;
- La strumentazione utilizzata deve essere custodita con cura evitando ogni possibile forma di danneggiamento;
- E' sconsigliato vivamente l'inserimento di dati personali all'interno dei computer dati in uso per le finalità del presente articolo in quanto possono essere visionati e trattati da altri utenti. In ogni caso la responsabilità dei dati inseriti è interamente a carico del soggetto cui è stata consegnata la strumentazione a cui spetta il compito della loro cancellazione al termine del corso e/o della manifestazione;
- La strumentazione va sempre riposta all'interno delle apposite custodie. Prima di riporre il videoproiettore è necessario far raffreddare la lampada onde evitare che si danneggi;

- La strumentazione non può essere lasciata incustodita neanche all'interno dei locali comunali, pertanto, una volta conclusa la manifestazione per la quale se ne è chiesto l'utilizzo, essa va immediatamente riconsegnata agli addetti comunali o, in caso di impossibilità, deve essere restituita entro le ore 8,30 del primo giorno lavorativo successivo alla data della manifestazione;
- Qualora il corso o la manifestazione vengano svolti presso la sala Capitini la strumentazione può essere riposta all'interno dell'apposto armadietto le cui chiavi vanno riconsegnate entro le 8.30 del primo giorno lavorativo successivo alla data del corso / manifestazione.

Art. 34
Utilizzo di internet per manifestazioni, corsi ed eventi in generale

1. L'utilizzo di internet nelle sale comunali è soggetto a tutte le disposizioni del presente regolamento e può avvenire solo previa richiesta scritta al Sistema Informatico che provvederà nei limiti dei sistemi presenti all'interno dell'Ente ad assegnare le credenziali necessarie allo svolgimento di detta attività (indirizzo IP oppure user e password).
Qualora la richiesta venga fatta per manifestazioni non organizzate direttamente dall'Ente è necessaria autorizzazione scritta da parte del Sindaco o della Giunta Comunale.

3. Al momento della consegna delle credenziali di accesso chi effettua la richiesta dovrà sottoscrivere apposito documento nel quale si dichiara direttamente responsabile, civilmente e penalmente a norma delle vigenti leggi delle attività svolte durante la connessione ad internet e prende visione sottoscrivendole delle disposizioni degli artt. 30, 31 e 32.

Capo VI
-
ALTRI SERVIZI

Art. 35
Misure adottate in caso di assenza del lavoratore

1. Le credenziali di cui all'Art 21 hanno anche la funzione di impedire l'accesso di altri alla parte dell'hard disk contenente i dati dell'utente. E' vietato comunicare le proprie credenziali ad altri in quanto tale comportamento espone al rischio, tra l'altro, di permettere l'accesso ai propri dati in caso di assenza.

2. Nel caso in cui si renda necessario accedere ai dati presenti esclusivamente nel PC dell'incaricato e questi risulti assente, si seguirà la seguente procedura per permettere l'accesso ai dati e la continuazione del lavoro:

a) il responsabile di riferimento a cui appartiene l'incaricato avanza richiesta scritta e motivata in cui è dettagliatamente indicato il file o la cartella alla quale si intende accedere. La richiesta va indirizzata al responsabile del Sistema Informatico;

b) il responsabile di riferimento o in sua assenza il responsabile del Sistema Informatico, autorizzano la modifica della password dell'incaricato assente in modo da permettere l'accesso alla sua postazione. Non è tecnicamente possibile, per il Sistema Informatico, conoscere le password degli utenti ma è possibile modificarle;

c) il responsabile di riferimento a cui appartiene l'incaricato riceve dal funzionario responsabile del Sistema Informatico la nuova password così come modificata, ed effettua, o fa effettuare ad altri utenti appositamente delegati per iscritto, l'accesso alla postazione dell'incaricato assente potendo prelevare solo i file e le cartelle descritte nella richiesta. Il responsabile o suo delegato provvede alla modifica immediata della password. Ogni altro accesso costituisce un trattamento illecito dei dati con ogni conseguenza penale, civile e amministrativa;

d) il responsabile di riferimento a cui appartiene l'incaricato assente provvede ad avvisare prontamente lo stesso circa l'avvenuto accesso alla sua postazione, invitandolo a modificare immediatamente la password al suo ritorno;
e) l'incaricato assente modificherà la password immediatamente al suo ritorno impedendo così successivi accessi alla sua postazione.

Art. 36
Ingressi/uscita di personale dalla struttura organizzativa dell'Ente

1. I Responsabili di settore e/o l'ufficio del personale hanno l'obbligo di comunicare l'ingresso, la variazione di mansione o uscita dalla struttura organizzativa di personale, sia esso subordinato, parasubordinato, con prestazione volontaria (esempio stagisti o servizio civile volontario), o con prestazione professionale, almeno 48 ore prima dei suddetti ingressi, variazioni o uscite.

2. La comunicazione deve essere formalizzata agli addetti preposti alla gestione delle politiche di sicurezza delle informazioni (responsabile del Sistema Informatico, Amministratori di Sistema e/o qualsiasi altro soggetto individuato quale referente di una procedura anche se gestita esternamente all'Ente). Tali soggetti, secondo la normativa ed i regolamenti applicabili, provvederanno all'aggiornamento delle credenziali degli utenti all'interno dei sistemi e alla revisione del modello sul trattamento delle banche dati allegato al Documento programmatico sulla sicurezza.

3. E' altresì fatto divieto far utilizzare credenziali utente di terzi a chiunque, in modo particolare a parasubordinati, collaboratori volontari e prestatori d'opera.

4. Il responsabile del Sistema Informatico e gli Amministratori di sistema non sono responsabili di quanto accade per effetto dell'utilizzo di credenziali di accesso che non siano state da esso assegnate (es. sistemi gestiti esternamente all'ente) né da utilizzi impropri delle stesse;

5. Ne consegue che, nel caso ricorra quanto previsto al comma 4 del presente articolo, qualunque azione è a totale responsabilità di chi la esegue e di chi ha consentito che questa potesse avere effetto (personale dell'Ente in possesso di credenziali, sia esso subordinato, parasubordinato, con prestazione volontaria - esempio stagisti o servizio civile volontario - o con prestazione professionale senza e del Responsabile del Sistema Informatico), che ne rispondono amministrativamente, civilmente e penalmente, secondo le norme applicabili.

Art. 37
Controlli sull'uso della strumentazione

1. L'Amministrazione ha il diritto di verificare, tramite gli strumenti tecnici disponibili, l'effettivo utilizzo che viene fatto delle proprie attrezzature.
Nell'effettuazione di questi controlli dovranno comunque essere rispettati i diritti alla privacy dei dipendenti sanciti dalle normative vigenti.
Non potranno in alcun caso essere registrate le telefonate effettuate e non potrà essere visionata la posta, cartacea o elettronica, inviata o ricevuta all'indirizzo personale del dipendente. Non potranno essere inoltre esaminati all'insaputa del dipendente i contenuti degli archivi presenti sulla sua stazione di lavoro, tranne che nei casi previsti dalla legge e su richiesta della magistratura.
Potrà invece essere tenuta traccia dei numeri telefonici utilizzati, della durata delle chiamate, degli indirizzi di mail usati, delle pagine internet visitate, ed in generale delle risorse su Internet utilizzate.
Le informazioni raccolte a questo scopo potranno essere visionate esclusivamente dal responsabile o da suoi incaricati e dovranno essere distrutte dopo tre mesi, sempre che non abbiano dato luogo a provvedimenti disciplinari; in questo caso dovranno essere distrutte una volta terminato il procedimento in questione.

Art. 38
Deroghe

1. Tutte le norme di sicurezza sopra indicate e relative all'uso di attrezzature, servizi o software non si applicano al personale del Servizio Informatico in quanto fa parte dei compiti di tale ufficio la sperimentazione di nuovi software o la ricerca di vulnerabilità e pericoli potenziali che potrebbero essere presenti nelle infrastrutture messe a disposizione.
2. Per quanto riguarda l'accesso ai dati personali degli utenti, sono fatte salve le prerogative degli addetti al Servizio "Informatica comunale" e comunque degli addetti alla manutenzione delle apparecchiature, che sono comunque tenuti a limitare l'accesso a tali informazioni allo stretto indispensabile ed a rispettare i vincoli di riservatezza.

Art. 39
Conseguenze per utilizzi indebiti

1. È fatto obbligo a tutti gli utenti 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 dal vigente CCNL nonché con tutte le azioni civili e penali consentite.

   Si rammenta che il potere disciplinare non può comunque essere esercitato nei confronti dei collaboratori coordinati e continuativi, dei collaboratori a progetto e dei tirocinanti, mentre nei confronti dei lavoratori somministrati (ex interinali) va esercitato per il tramite dell'agenzia di somministrazione.
   Con riferimento ai collaboratori, qualora questi per l'espletamento del loro incarico si servissero degli strumenti aziendali considerati dal Regolamento, si propone di prevedere nell'ambito del contratto a progetto l'obbligo per il collaboratore di rispettare il Regolamento in questione, con diritto della Committente, nei casi di violazione di particolare gravità, di risolvere il contratto stesso.

2. I costi di beni, servizi e di personale necessari per il ripristino della situazione "quo ante" derivante da un uso improprio delle strumentazioni in uso o in violazione del presente Regolamento da parte del personale saranno addebitati ai trasgressori.

Art. 40
Sanzioni per inosservanza delle norme

1. Le presenti istruzioni sono impartite ai sensi delle normative vigenti in materia di privacy, l'inosservanza delle quali da parte dell'incaricato può comportare sanzioni anche di natura penale a suo carico ai sensi delle disposizioni di cui alla parte III, titolo III, capi I e II del D.Lgs. n. 196/2003.