CITTÀ DI CORBETTA

# REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI

APPROVATO CON DELIBERAZIONE DI GIUNTA COMUNALE N. 55 DEL 26.4.2012

## Sommario

## Premessa

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet dai Personal Computer, espone il Comune di Corbetta ai rischi di un coinvolgimento sia patrimoniale sia penale, creando problemi alla sicurezza e all'immagine dell'Ente stesso.

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

Inoltre le recenti disposizioni emanate dall'Autorità Garante, mediante il provvedimento di carattere generale del 1 Marzo 2007 (Del. N. 13 del 1/3/2007), in cui vengono definite le linee guida per l'utilizzo della posta elettronica ed Internet impongono l'adozione di precise e definite regole per l'utilizzo di tali strumenti.

## Utilizzo del Personal Computer

Il Personal Computer affidato al dipendente è uno *strumento di lavoro.* Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Il personale deve custodire la propria strumentazione in modo appropriato e diligente, segnalando tempestivamente ogni danneggiamento, furto o smarrimento al proprio responsabile di servizio.

L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata, se non al custode della password con le modalità definite dal Documento Programmatico per la Sicurezza vigente. La stessa password deve essere attivata per l'accesso alla rete, per lo screen saver e per il collegamento a Internet.

Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte del Responsabile dei sistemi informatici.

Il Responsabile del Servizio C.E.D. e lo staff da lui diretto, per l'espletamento delle funzioni e mansioni assegnate, ha la facoltà di monitorare lo spazio occupato dalle caselle di posta elettronica sul server e informare gli utilizzatori circa l'opportunità di liberare spazio, cancellando alcuni messaggi, quando lo spazio libero si approssima a zero.

Il custode delle parole chiave riservate**,** per l'espletamento delle sue funzioni, ha la facoltà in qualunque momento di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica interna ed esterna.

Il custode delle parole chiave riservate potrà accedere ai dati ed agli strumenti informatici esclusivamente per permettere allo stesso Ente, titolare del trattamento, di accedere ai dati trattati da ogni incaricato con le modalità fissate dallo stesso Ente, al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività del Comune nei casi in cui si renda indispensabile ed indifferibile l'intervento, ad esempio in caso di prolungata assenza od impedimento dell'incaricato, informando tempestivamente l'incaricato dell'intervento di accesso realizzato.

Non è consentito installare autonomamente programmi provenienti dall'esterno senza la preventiva autorizzazione del Responsabile dei sistemi informatici ed una richiesta scritta da parte del dirigente responsabile dell'unità cui è assegnato il PC. In caso di necessità di acquisto o dotazione di software applicativi e/o procedure pertinenti esclusivamente alcune aree ed i relativi dirigenti, deve essere comunque richiesta per iscritto l'autorizzazione preventiva da parte del Responsabile del Servizio Sistemi Informativi, per garantire la compatibilità funzionale, tecnica ed il mantenimento dell'efficienza operativa dei sistemi e delle reti. Sussiste infatti il grave pericolo di introdurre involontariamente virus informatici o di alterare la stabilità delle applicazioni degli elaboratori e dei sistemi operativi.

Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dal responsabile dei sistemi informatici del Comune di Corbetta.

L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'Ente a gravi responsabilità civili ed anche penali in caso di violazione

della normativa a tutela dei diritti d'autore sul software (D. Lgs. 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore) che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore.

Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, i punti rete di accesso, le configurazioni delle reti LAN/WAN presenti nelle sedi e la configurazione del Browser per la navigazione, salvo autorizzazione esplicita del Responsabile del Servizio Sistemi Informativi.

E' responsabilità del dirigente verificare il coerente utilizzo delle risorse assegnate ed evitarne l'uso improprio o l'accesso alle risorse da parte di personale non autorizzato, compreso l'utilizzo da parte di terzi di punti rete in luoghi non presidiati.

Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. 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. In ogni caso deve essere attivato lo screen saver e la relativa password.

Non è consentita l'installazione sul proprio PC o il collegamento sulla rete LAN di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, pc portatili, telefoni cellulari, PDA ed apparati in genere), se non con l'autorizzazione espressa del Responsabile dei sistemi informatici, previa richiesta scritta da parte del dirigente responsabile dell'unità cui è assegnato il PC o il segmento di rete LAN.

Agli utenti incaricati del trattamento dei dati sensibili è fatto obbligo di distruggere eventuali copie di sicurezza o supporti di tipo removibile (floppy, CDRom, Nastri) quando gli stessi non sono più utilizzati, al fine di rendere irrecuperabili i dati in essi contenuti. Ai sensi del Dlgs 196/03 è fatto divieto di divulgazione a qualsiasi titolo delle informazioni presenti nelle banche dati dell'ente se non disciplinate da appositi protocolli di intesa.

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il Responsabile del Servizio Sistemi Informativi nel caso in cui siano rilevati virus ed adottando quanto previsto dal successivo punto del presente Regolamento relativo alle procedure di protezione antivirus nella sezione "Protezione Antivirus".

Non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

E' vietato rimuovere, danneggiare deliberatamente o asportare componenti hardware.

E' vietato accedere direttamente ad Internet con modem collegato al proprio Personal Computer se non espressamente autorizzati e per particolari motivi tecnici.

E' vietato utilizzare gli strumenti informatici comunali al fine di custodire, far circolare o promuovere materiale pubblicitario personale, codice maligno (virus, trojan horses, programmi pirata o altre porzioni di codice maligno e/o altro materiale non autorizzato).

E' vietato 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.

## Utilizzo della rete del Comune di Corbetta

Hanno diritto ad accedere alla rete del Comune di Corbetta tutti i dipendenti, gli amministratori, le ditte fornitrici di software e/o servizi per motivi di manutenzione e limitatamente alle applicazioni di loro competenza, collaboratori esterni impegnati nelle attività istituzionali per il periodo di collaborazione.

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità, vengono svolte regolari attività di controllo, amministrazione e backup.

Le password d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.

È assolutamente proibito entrare nella rete e nei programmi con altri nomi utente.

Il Responsabile dei sistemi informatici può in qualunque momento procedere alla rimozione di ogni file o

applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.

Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante.

E' vietato installare o eseguire deliberatamente o diffondere su qualunque computer e sulla rete, programmi destinati a danneggiare o sovraccaricare i sistemi o la rete (p.e. virus, cavalli di troia, worms, spamming della posta elettronica, programmi di file sharing - p2p.)

E' vietato monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività degli utenti, leggere copiare o cancellare file e software di altri utenti, senza averne l'autorizzazione esplicita.

E' vietato usare l'anonimato o servirsi di risorse che consentano di restare anonimi sulla rete.

## Utilizzo delle stampanti di rete

È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni. È buona regola evitare di stampare documenti o file non adatti (molto lunghi o non supportati, come ad esempio il formato pdf o file di contenuto grafico) su stampanti comuni. In caso di necessità la stampa in corso può essere cancellata.

## Gestione delle Password

Le password di ingresso alla rete, di accesso ai programmi e dello screen saver, sono previste ed attribuite dal Responsabile dei sistemi informatici.

È necessario procedere alla modifica della password a cura dell'incaricato del trattamento al primo utilizzo e, successivamente, almeno ogni sei mesi; nel caso di trattamento di dati sensibili e di dati giudiziari la periodicità della variazione deve essere ridotta a tre mesi (come previsto dal punto 5 del disciplinare tecnico allegato al Codice della privacy, d.lgs.vo n.196/2003) con contestuale comunicazione al Custode delle credenziali di autorizzazione in busta chiusa.

Le password possono essere formate da lettere (maiuscole o minuscole) e numeri ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema; devono essere composte da almeno dieci caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato (punto 5 del disciplinare tecnico).

La password deve essere immediatamente sostituita, dandone comunicazione al Custode delle credenziali di autorizzazione, nel caso si sospetti che la stessa abbia perso la segretezza.

Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia al Titolare o persona dalla stessa incaricata

## Utilizzo dei supporti magnetici

Tutti i supporti magnetici riutilizzabili (dischetti, cassette, cartucce) contenenti dati sensibili e giudiziari devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato (punto 22 del disciplinare tecnico). Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.

In caso di dismissione, per evitare problemi di sicurezza, questi supporti dovranno essere consegnati al Responsabile del sistema informatico così da permettere una loro corretta distruzione.

I supporti magnetici contenenti dati sensibili e giudiziari (punto 21 del disciplinare tecnico) devono essere custoditi in armadi ignifughi chiusi a chiave o in cassaforte.

Non è consentito scaricare files contenuti in supporti magnetici/ottici non aventi alcuna attinenza con la propria prestazione lavorativa.

Tutti i files di provenienza incerta, ancorché potenzialmente attinenti all'attività lavorativa, non devono essere utilizzati/installati/testati. Nel caso di effettiva necessità di impiego devono essere sottoposti ad un preventivo controllo ed alla relativa autorizzazione all'utilizzo da parte del Responsabile del Servizio Sistemi Informativi e/o del suo staff tecnico

## Utilizzo di Personal Computer portatili

L'utente è responsabile del Personal Computer portatile assegnatogli da Responsabile dei sistemi informatici e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Ai PC portatili si applicano le regole di utilizzo previste per i PC connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.

I PC portatili ed ogni apparecchio elettronico ceduto in uso dal Comune di Corbetta al dipendente, utilizzati all'esterno (convegni, fiere, ecc…), in caso di allontanamento, devono essere custoditi in un luogo protetto.

Eventuali configurazioni di tipo Accesso Remoto, dirette verso la rete aziendale o attraverso internet, devono essere autorizzate esclusivamente a cura del Responsabile del Servizio Sistemi Informativi. E' vietato utilizzare le suddette connessioni all'interno delle sedi comunali se contemporaneamente connessi alla rete LAN.

## Uso della posta elettronica

La casella di posta, assegnata dall'Azienda all'utente, è uno **strumento di lavoro**. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

È fatto divieto di utilizzare le caselle istituzionali di posta elettronica dell'Ente ***……@comune.corbetta.mi.it*** per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list salvo diversa ed esplicita autorizzazione.

È buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

E' previsto un dimensionamento massimo per ciascuna casella pari a 250 MB, di questo spazio è buona norma non superare il 70-80%.

Non è possibile modificare i criteri di archiviazione delle caselle di posta elettronica.

Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o pre-contrattuali per il Comune di Corbetta deve essere visionata od autorizzata dal responsabile di settore, o in ogni modo è opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria.

La documentazione elettronica che costituisce per l'Ente "know how" tecnico protetto (tutelato in base all'art. 6 bis del r.d. 29.6.1939 n.1127), e che, quindi, viene contraddistinta da diciture od avvertenze dirette ad evidenziarne il carattere riservato o segreto a tutela del patrimonio dell'Ente, non può essere comunicata all'esterno senza preventiva autorizzazione del responsabile di settore.

È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario, ma di norma per la comunicazione ufficiale è obbligatorio avvalersi degli strumenti tradizionali (fax, posta, …).

Per la trasmissione di file all'interno del Comune di Corbetta è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati.

È obbligatorio controllare i file attachements di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

È vietato inviare catene telematiche (o di Sant'Antonio). Se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente all' Responsabile dei sistemi informatici. Non si devono in alcun caso attivare gli allegati di tali messaggi.

Saranno messe a disposizione dei singoli incaricati le funzionalità del software di gestione della posta elettronica, che consentiranno, qualora ci dovessero essere assenze programmate, di inviare, in automatico, messaggi di risposta che contengano le "coordinate" di altro soggetto o strutture del Comune di Corbetta operanti al posto del lavoratore assente.

Qualora dovesse rendersi necessario conoscere il contenuto dei messaggi di posta elettronica in caso di assenza prolungata od improvvisa e/o per improrogabili necessità legate all'attività lavorativa, l'incaricato dovrà individuare un proprio collega "fiduciario" il quale provvederà a verificare il contenuto dei messaggi. In caso di mancata individuazione sarà cura del responsabile del settore/servizio o del Direttore generale procedete a tale nomina.

Di tale attività sarà redatto un verbale ed informato tempestivamente alla prima occasione utile il lavoratore interessato.

Si evidenzia che, qualora dovessero rendersi necessari dei controlli sull'uso degli strumenti elettronici da parte dei lavoratori saranno rispettati i principi di pertinenza e non eccedenza e saranno evitate ingiustificate interferenze sui diritti e sulle libertà fondamentali dei lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata. In tal senso eventuali esigenze connesse ad azioni mirate di controllo saranno effettuate in maniera graduale, riguardando in prima istanza dati aggregati, riferiti all'intera struttura lavorativa o sue specifiche aree, richiamando le stesse ad utilizzo pertinente degli strumenti informatici posti a loro disposizione. Qualora gli esiti dovessero generare l'assenza di successive anomalie saranno effettuati controlli di carattere generale.

Si precisa altresì che tali controlli non saranno effettuati in maniera prolungata, costante o indiscriminata, ma mirati ad individuare eventi dannosi o situazioni di pericolo per le quali non sia stato possibile impedirne gli effetti attraverso preventivi accorgimenti tecnici.

## Uso della rete Internet e dei relativi servizi

Per ragioni di sicurezza e per garantire l'integrità dei sistemi informatici, l'accesso ad Internet effettuato tramite elaboratori connessi alla rete comunale è scrupolosamente protetto da appositi dispositivi di sicurezza informatica (fìrewall, viruswall, antivirus, proxy server, etc.).

Il Comune di Corbetta, inoltre si è dotato di una soluzione software per la riduzione dei rischi associati all'utilizzo delle applicazioni desktop, di rete e Internet da parte dei dipendenti comunali, al fine di consentire il miglioramento della produttività e della sicurezza informatica, oltre che salvaguardare le risorse IT e ridurre i rischi di responsabilità legale.

Tale soluzione permette di gestire l'accesso a Internet da parte dei dipendenti attraverso un sistema di "filtraggio e di controllo" delle richieste di navigazione, di bloccare la condivisione di file peer-to-peer, di impedire il funzionamento di programmi spia e di gestire l'utilizzo di applicazioni a elevato consumo di banda, quali, ad esempio, il download di file audio e video, e consente di salvaguardare l'immagine e le responsabilità aziendali bloccando l'accesso ai siti Internet dai contenuti discutibili o dispersivi, di mantenere alta la produttività individuale e, di conseguenza, quella generale, ma, soprattutto di evitare consumi inutili di traffico in Internet.

Si evidenzia che, qualora dovessero rendersi necessari dei controlli sull'uso di Internet da parte dei lavoratori, saranno rispettati i principi di pertinenza e non eccedenza e saranno evitate ingiustificate interferenze sui diritti e sulle libertà fondamentali dei lavoratori. In tal senso eventuali esigenze connesse ad azioni mirate di controllo saranno effettuate in maniera graduale, riguardando in prima istanza dati aggregati, riferiti all'intera struttura lavorativa o gruppi sufficientemente ampi di lavoratori tali da precludere l'immediata identificazione degli utenti (ad es., con riguardo ai *file* di *log* riferiti al traffico).

Si precisa altresì che tali controlli non saranno effettuati in maniera prolungata, costante o indiscriminata, ma mirati ad individuare eventi dannosi o situazioni di pericolo per le quali non sia stato possibile impedirne gli effetti attraverso preventivi accorgimenti tecnici. Per questi motivi il Comune di Corbetta ha provveduto ad installare un software (detto comunemente web filter) che prevenga determinate operazioni, reputate inconferenti con l'attività lavorativa, quali l'upload o l'accesso a determinati siti (inseriti in una sorta di black list) e/o il download di file o software aventi particolari caratteristiche (dimensionali o di tipologia di dato). La conservazione dei dati riguardanti l'uso degli strumenti elettronici è regolata in modo che venga

automaticamente effettuata la sovraregistrazione dei file, e vengano in tal maniera cancellati periodicamente ed automaticamente i dati personali la cui conservazione non sia necessaria.

Un eventuale prolungamento dei tempi di conservazione va valutato come eccezionale e può aver luogo solo in relazione :

- ad esigenze tecniche o di sicurezza del tutto particolari
- all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria
- all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

Il Personal Computer abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. È assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.

È fatto divieto all'utente lo scarico e comunque l'installazione di software prelevato da siti Internet o da altre fonti, se non espressamente autorizzato dal Responsabile dei sistemi informatici.

Non è consentito lo scarico di materiale elettronico tutelato dalle normative sul Diritto d'Autore (software, file audio, film, etc.) né attraverso Internet, né attraverso servizi peer-to-peer.

È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dai responsabili di settore e con il rispetto delle normali procedure di acquisto.

È da evitare ogni forma di registrazione a siti, mailing-list i cui contenuti non siano legati all'attività lavorativa.

È vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

Non è consentita la navigazione in siti ove sia possibile rivelare le opinioni politiche, religiose o sindacali dell'utilizzatore; non è consentito inoltre visitare siti e memorizzare documenti informatici dai contenuti di natura oltraggiosa e/o discriminatoria per sesso/etnia/religione/opinione e/o appartenenza sindacale e/o politica.

## Protezione antivirus

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

Ogni utente è tenuto a controllare il regolare funzionamento e l'aggiornamento periodico del software installato, secondo le procedure previste.

Nel caso che il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente:

a) sospendere ogni elaborazione in corso senza spegnere il computer

b) segnalare l'accaduto al Responsabile del Servizio Sistemi Informativi.

Non è consentito l'utilizzo di floppy disk, cd rom, cd riscrivibili, nastri magnetici di provenienza ignota.

Ogni dispositivo magnetico di provenienza esterna all'azienda dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere consegnato al Responsabile del Servizio Sistemi Informativi.

## Osservanza delle disposizioni in materia di Privacy

È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, come indicate nella lettera di designazione di incaricato del trattamento dei dati ai sensi del disciplinare tecnico allegato al d.lgs.vo n. 196/2003.

## Non osservanza della normativa dell'Ente

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

## Aggiornamento e revisione

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dall'Ente.

Il presente Regolamento è soggetto a revisione con frequenza annuale.

Il presente regolamento viene consegnato a ciascun dipendente/utilizzatore del Comune di Corbetta. Il dipendente deve attenersi, nell'utilizzo e nella gestione delle risorse strumentali informatiche comunali, ai principi e ai doveri stabiliti nel "Codice di comportamento dei dipendenti delle pubbliche amministrazioni". (D. M. 31 marzo 1994 - Ministero per la Funzione Pubblica)

La violazione da parte dei lavoratori dei principi e delle norme contenute nel presente regolamento costituisce violazione degli obblighi e dei doveri del dipendente pubblico e, pertanto, in relazione alla gravità dell'infrazione, i dirigenti responsabili, previo espletamento di procedimento disciplinare, possono procedere

all'applicazione delle sanzioni previste dalle disposizioni contrattuali vigenti in materia.