TITOLARE DEL TRATTAMENTO
Comune di Castelfranco Veneto

DISCIPLINARE PER L'UTILIZZO DEGLI STRUMENTI ELETTRONICI, POSTA ELETTRONICA, INTERNET, TELEFONI E FAX DEL COMUNE

INDICE

PREMESSA

La diffusione ed utilizzazione delle tecnologie informatiche, telematiche e digitali in genere, in particolare l'accesso alla rete Internet, espone il Comune di Castelfranco Veneto a rischi di un coinvolgimento sia patrimoniale che civile o penale, creando problemi alla sicurezza e all'immagine dell'Amministrazione stessa.

Il Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione di dati personali", impone comportamenti tali da assicurare a chiunque il diritto alla protezione dei dati personali che lo riguardano.

Il Garante per la protezione dei dati personali ha emanato, in data 01.03.2007, un provvedimento in materia di lavoro denominato "Lavoro:le linee guida del Garante per posta Elettronica e Internet", con il quale prescrive ai datori di lavoro di adottare la misura necessaria a garanzia degli interessati, riguardante l'onere di specificare le modalità di utilizzo della posta elettronica e della rete internet da parte dei lavoratori, indicando chiaramente le modalità di uso degli strumenti messi a disposizione e se, in che misura e con quali modalità vengono effettuati controlli.

Premesso quindi che l'utilizzo delle risorse informatiche, digitali e telematiche della nostra Amministrazione deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, il Comune di Castelfranco Veneto adotta attraverso il presente disciplinare delle regole interne dirette ad evitare che condotte inconsapevoli possano innescare problemi e minacce alla sicurezza nel trattamento dei dati oltre che determinare un utilizzo improprio degli strumenti informatici.

Il presente Disciplinare si prefigge pertanto di tutelare gli interessi dell'Amministrazione ed al contempo la riservatezza dei dati personali dei Lavoratori rispetto all'uso degli strumenti elettronici, posta elettronica, internet, telefoni aziendali e fax.

Il presente disciplinare si applica a:

a) Dirigenti e dipendenti, a qualsiasi titolo inseriti nell'organizzazione comunale, senza distinzione di ruolo e/o livello;

b) Collaboratori dell'Amministrazione comunale, a prescindere dal rapporto contrattuale intrattenuto con la stessa.

1) TRATTAMENTI DI DATI EFFETTUATI CON STRUMENTI INFORMATICI, TELEMATICI E DIGITALI IN GENERE

Tutti i trattamenti di dati, compresi quelli effettuati con strumenti informatici, telematici e digitali in genere, svolti in nome e per conto del Comune di Castelfranco Veneto, devono essere connessi alla realizzazione di procedimenti amministrativi e/o per le legittime finalità istituzionali perseguite dalla Pubblica Amministrazione medesima.

I trattamenti dei dati personali svolti in nome e per conto del Comune di Castelfranco Veneto, sono effettuati da Incaricati del trattamento dei dati, nominati dai Responsabili del Trattamento dei dati.

Il Comune di Castelfranco Veneto provvede ad assegnare un nome utente e parola chiave (user-id e password) con i relativi profili d'autorizzazione, ad ogni incaricato che effettua un trattamento dati con strumenti informatici, telematici e digitali in genere. Provvede inoltre all'applicazione di ogni altra misura di sicurezza prevista dalla normativa vigente o comunque ritenuta necessaria.

Preposti al trattamento strumentale dei sistemi informatici del Comune di Castelfranco Veneto sono gli Amministratori di Sistema nominati tra il personale del Comune e/o tra altri soggetti esterni in virtù di impegni assunti di norma su basi contrattuali.

2) UTILIZZO DEL PERSONAL COMPUTER E DEGLI ARCHIVI INFORMATICI

Il Personal Computer (P.C.) affidato al dipendente, anche temporaneamente, è uno strumento di lavoro. L'uso improprio dello strumento può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

L'accesso all'elaboratore, alla rete di elaboratori ed alle procedure informatiche (programmi) è protetto da user-id e password con associati i profili di autorizzazione (credenziali di autenticazione), diverse per ogni utente, che devono essere custodite dall'incaricato con la massima diligenza e rimanere segrete. La stessa password per l'accesso al P.C. deve essere attivata per lo screen saver.

Gli archivi informatici di qualsiasi natura (siano essi organizzati, indicizzati o semplici contenitori di informazioni, come ad es. documenti Word, fogli excel, ecc.) sono anch'essi strumenti di lavoro. Ogni utilizzo non inerente all'attività istituzionale dell'ente è vietato. Agli archivi informatici, indipendentemente da chi è il creatore o il titolare, possono accedere tutti i Responsabili o Incaricati al trattamento muniti di idoneo profilo di autorizzazione, solo per svolgere le operazioni connesse al loro incarico.

Il sistema informatico del Comune di Castelfranco Veneto si compone di più server e più client (P.C.), con più sedi distaccate collegate attraverso varie modalità, con cartelle condivise e cartelle personali residenti sui client o sui server. Sia le cartelle condivise che quelle personali possono contenere solo dati relativi all'attività del Comune di Castelfranco Veneto.

Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dagli Amministratori di sistema, salvo preventiva autorizzazione degli Amministratori di sistema stessi. L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre la Pubblica Amministrazione a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore. Gli Amministratori di sistema possono in qualunque momento procedere alla rimozione di applicazioni o programmi che si ritengano essere pericolosi per la Sicurezza ed integrità del sistema informativo.

Il P.C., salvo diversa disposizione, deve essere spento a fine giornata o prima di lasciare gli uffici. In caso di allontanamento, anche temporaneo, dalla postazione di lavoro deve essere verificato che non vi sia la possibilità da parte di terzi di accedere ai dati personali utilizzando il P.C. e pertanto deve essere attivato lo screen saver con password.

Non è consentita l'installazione sul proprio P.C. di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, …), se non con l'autorizzazione espressa degli Amministratori di sistema. Non è consentito nessuna installazione di hardware o apparati o interventi sulle reti informatiche comunali nel sistema informatico Comunale senza l'autorizzazione degli Amministratori di Sistema.

Il sistema informatico del Comune di Castelfranco Veneto è protetto da un software antivirus centralizzato che distribuisce gli aggiornamenti sui client; ogni Incaricato del trattamento deve prestare la

massima attenzione alle eventuali segnalazioni avvisando immediatamente il personale del servizio "Sistemi Informativi" nel caso in cui vengano rilevati programmi maligni (comunemente detti virus, worms, trojan horse, malicious codes e simili) o nel caso rilevi qualche anomalia nel funzionamento dell'antivirus.

È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni.

Tutti gli Incaricati del trattamento sono tenuti ad effettuare le copie di back-up (salvataggio) dei dati secondo le istruzioni impartite con l'apposita circolare.

3) GESTIONE DELLE CREDENZIALI DI AUTENTICAZIONE

Le credenziali di autenticazione, tipicamente user-id e password (utente e parola-chiave), con i relativi profili di autorizzazione associati, sono diverse per ogni incaricato del trattamento e vengono utilizzate per l'accesso al P.C., alla rete e ai programmi, oltre che ad altri apparati elettronici; sono attribuite dagli Amministratori di sistema ad ogni Incaricato del trattamento, su richiesta scritta del Responsabile del trattamento competente che nomina l'Incaricato al trattamento. Il Responsabile del trattamento provvederà a richiedere la disattivazione della password o la variazione dei profili di autorizzazione in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali;

Le passwords devono essere custodite dall'incaricato con la massima diligenza e non devono essere comunicate a nessuno.

Le passwords debbono avere caratteristiche di complessità (D.Lgs. 196/2003 – Allegato B punto 5): questo significa che debbono essere formate da lettere (maiuscole o minuscole), numeri e simboli (almeno 3 di questi 4 requisiti); devono essere composte da almeno 8 caratteri oppure nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; non devono contenere riferimenti agevolmente riconducibili all'incaricato.

È necessario procedere alla modifica della password a cura dell'Incaricato del trattamento al primo utilizzo e, successivamente, almeno ogni 90 giorni, in quanto vi è un diffuso trattamento di dati sensibili o giudiziari . Qualora sia possibile, gli Amministratori di sistema provvedono a meccanismi automatici che impongono il cambio di password.

Alcuni sistemi non hanno la possibilità di combinare user-id e password per sistemi di riconoscimento dei vari utenti. Di conseguenza sono applicate delle password di sistema(BIOS).In questo caso l'accesso ai dati può essere eseguito esclusivamente mediante la conoscenza della password di sistema(BIOS), per cui quest'ultima deve essere consegnata in busta chiusa al "Custode delle password" designato e agli amministratori di sistema. L'Incaricato deve rivolgersi al Responsabile del trattamento per ottenere indicazioni sul Custode delle password designato. Tale operazione dovrà essere ripetuta ogni 3 mesi in corrispondenza della modifica della password da parte dell'incaricato. Le buste verranno aperte dal "custode delle password" e le password utilizzate solo in caso di assoluta ed improrogabile necessità di avere la disponibilità dei dati che non sono altrimenti consultabili, comunicando tempestivamente al proprietario della password dell'utilizzo di quest'ultima, che provvederà ad un cambio immediato della stessa.
Ovviamente, con l'utilizzo di sistemi che consentono un'autenticazione riservata per ogni incaricato, non sarà necessario ricorrere alla figura del "custode delle password". In questo caso per rendere disponibili i dati contenuti ad es. in quel P.C. o in cartelle residenti sui server per i motivi previsti e di seguito specificati, il Responsabile del trattamento competente chiederà per iscritto agli Amministratori di sistema, di avere la disponibilità dei dati. Il Responsabile del trattamento competente dovrà avvisare tempestivamente il proprietario della variazione della password o delle abilitazioni intervenute per rendere disponibili i dati.

Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte degli Amministratori di sistema.

Più in generale quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante la componente riservata della credenziale per l'autenticazione (quando l'accesso ai dati non può essere effettuato se non con l'unica password), la procedura suddetta deve essere eseguita, consegnando la busta chiusa con le credenziali di autenticazione al custode delle password designato dal Responsabile del trattamento e agli amministratori di sistema.

La password deve essere immediatamente sostituita nel caso si sospetti che la stessa abbia perso la caratteristica di segretezza.

Gli Amministratori di sistema designati**,** per l'espletamento delle proprie funzioni o su richiesta scritta del Responsabile del trattamento, hanno la facoltà in qualunque momento di accedere alle credenziali di autenticazione con i profili di autorizzazione degli incaricati e ai dati trattati dagli incaricati per i seguenti motivi:

- motivi legati alla manutenzione-gestione dei sistemi, avendo cura di svolgere operazioni strettamente necessarie al perseguimento delle relative finalità;
- in casi di necessità derivanti da eventi dannosi o situazioni di pericolo che pregiudichino l'integrità ed il corretto funzionamento del sistema informativo;
- su richiesta scritta del Responsabile del trattamento per permettere di accedere ai dati trattati dagli Incaricati al fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività istituzionale nei casi in cui si renda indispensabile ed indefferibile l'intervento; il Responsabile del trattamento competente dovrà avvisare tempestivamente il proprietario della variazione apportata alle credenziali di autenticazione per rendere disponibili i dati.

4) UTILIZZO DEI SUPPORTI MAGNETICI REMOVIBILI

L'uso di tutti i supporti magnetici (dischetti, cassette, cartucce, flash memory, CD ROM , DVD, ecc.), soprattutto se riutilizzabili, deve essere effettuato con estrema cautela onde evitare che il loro contenuto possa essere visionato da estranei o addirittura recuperato anche dopo la cancellazione. L'eventuale cancellazione o riutilizzo di supporti riscrivibili deve essere effettuata con procedure che non permettano in alcun modo il recupero delle informazioni cancellate.

I supporti removibili contenenti dati sensibili e giudiziari sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni, che, considerato il numero e la natura dei dati trattati, li rendano temporaneamente intelligibili anche a chi è autorizzato ad accedervi e permettano di identificare gli interessati solo in caso di necessità.

I supporti magnetici contenenti dati personali o a maggior ragione sensibili e giudiziari devono essere custoditi in archivi chiusi a chiave.

5) UTILIZZO DI PC PORTATILI

L'utente è responsabile del P.C. portatile assegnatogli dall'Amministrazione e deve custodirlo con diligenza sia durante gli spostamenti (dispositivi portatili) sia durante l'utilizzo nel luogo di lavoro.

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

I P.C. portatili utilizzati all'esterno (convegni, visite in azienda, ecc.), in caso di allontanamento, devono essere custoditi in un luogo protetto.

Possono essere autorizzati anche collegamenti in VPN o attraverso protocolli sicuri via Internet (ad esempio: https), o altri sistemi di collegamento a distanza, quando ritenuti compatibili con gli standard di sicurezza da parte degli Amministratori di sistema.

L'utilizzo di P.C. non di proprietà comunale connessi alla rete Lan/Man comunale deve essere autorizzato per scritto dagli Amministratori di sistema.

6) UTILIZZO DELLA POSTA ELETTRONICA

Le caselle di posta elettronica assegnate dal Comune all'utente, sia nominative che di Servizio/Ufficio, sono uno strumento di lavoro e le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

Le caselle di posta elettronica nominative sono assegnate all'utente su richiesta del Responsabile del trattamento dei dati; le caselle postali di Servizio/Ufficio sono accessibili previa autorizzazione del Responsabile del trattamento dei dati e possono essere condivise tra più utenti.

L'utilizzo della posta elettronica comunale è consentito solo per ragioni di servizio ed è consentito attraverso l'user-id e password (credenziali di autenticazione) assegnate ad ogni utente.

Non è permesso utilizzare le caselle di posta elettronica comunali per l'invio di messaggi personali o per la partecipazione a dibattiti, forum, mailing-list estranei al rapporto di lavoro, salvo diversa ed esplicita

autorizzazione. E' vietato aderire o rispondere a messaggi che invitano ad inoltrare e perpetuare verso ulteriori indirizzi e-mail contenuti o documenti oggetto delle cosiddette "catene di S. Antonio".

E' permesso l'utilizzo di caselle di posta elettronica diverse dai domini comunali per ragioni personali presso sistemi esterni (web-mail) non facenti parte del sistema di posta elettronica comunale, a patto che l'utilizzo sia estremamente moderato, corrispondente ad alcuni minuti nell'arco delle ore di lavoro e comunque con eventuali allegati estremamente leggeri, per non creare problemi alla funzionalità delle linee di connettività comunali.

L'Amministrazione può decidere a suo insindacabile giudizio di bloccare in qualsiasi momento l'accesso a siti con servizi che risultino pericolosi per la sicurezza del sistema informativo comunale.

Solo in caso di estrema necessità e urgenza i Lavoratori possono utilizzare le caselle di Posta Elettronica Comunale per motivi non attinenti all'attività lavorativa e, comunque, non in maniera ripetitiva e in modo estremamente moderato, veicolando eventuali allegati esclusivamente se estremamente leggeri. In tali casi limitati, le e-mail personali è opportuno siano contrassegnate con la menzione "Privato" o "Riservato" all'inizio dell'oggetto.

La documentazione elettronica è soggetta ai criteri di riservatezza, al pari della documentazione cartacea.

E' opportuno utilizzare la casella di posta elettronica ufficiale condivisa per l'invio e la ricezione di documentazione che è di interesse generale per il Servizio/ufficio.

È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario, ma in assenza di Caselle di Posta Certificata, tale conferma non ha valore giuridico, per cui in caso di comunicazioni ufficiali è necessario avvalersi degli strumenti tradizionali (fax, posta, ecc., secondo le indicazioni della Direzione).

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

L'invio di e-mail con allegati pesanti a mittenti multipli deve essere limitata al fine di evitare disfunzioni sul sistema di posta. Non deve essere usata la posta elettronica per scambiarsi files voluminosi tra gli uffici comunali.

E' fatto divieto in ogni caso, di trasmettere a chiunque a mezzo Posta Elettronica materiale di natura pedofilo/pornografico, fraudolento/illegale, blasfemo, molesto/osceno, collegato a gioco d'azzardo, discriminatorio per sesso, lingua, religione, razza, origine etnica, condizione di salute, opinione e appartenenza sindacale e/o politica.

Qualora la casella di posta elettronica non sia condivisa con altri lavoratori, Il lavoratore a cui è assegnata la casella postale in caso di assenza programmata è tenuto ad attivare le apposite funzionalità messe a disposizione che consentono di inviare automaticamente messaggi di risposta che avvisano il mittente dell'assenza del destinatario e individuano altre modalità di contatto con la struttura. In caso di eventuali assenze non programmate (ad. es. per malattia), qualora il dipendente non possa attivare la procedura descritta, il Responsabile del Trattamento, perdurando l'assenza oltre un determinato limite temporale, potrebbe disporre lecitamente, sempre che sia necessario e mediante il personale del servizio Sistemi Informativi, l'attivazione di un analogo accorgimento, avvertendo gli interessati.

In previsione della possibilità che, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica sia delle caselle postali nominative che delle caselle postali ufficiali, l'interessato deve delegare un altro lavoratore a verificare il contenuto dei messaggi e ad inoltrare al responsabile del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa; il responsabile del trattamento di tale attività informerà il lavoratore interessato alla prima occasione.

In caso di cessazione del rapporto di lavoro, il Responsabile del trattamento competente chiede il blocco agli amministratori di sistema designati della casella di posta elettronica del Lavoratore rendendo inagibile l'indirizzo e-mail.

7) USO DELLA RETE INTERNET E DEI RELATIVI SERVIZI

Internet costituisce uno strumento necessario allo svolgimento della propria attività lavorativa.

La navigazione in internet è permessa agli utenti mediante le credenziali di autenticazione assegnate all'utente attraverso un sistema di filtraggio denominato web-security.

È vietata la navigazione in Internet per motivi diversi da quelli legati all'attività lavorativa.

Eccezionalmente è permessa la navigazione in internet per motivi personali a patto che l'utilizzo sia estremamente moderato, corrispondente solo ad alcuni minuti nell'arco delle ore di lavoro giornaliere.

La navigazione in internet in qualsiasi caso non è consentita per :

- Attività che possono creare disservizio o danno all'Amministrazione;
- Attività poste in essere in violazione del diritto d'autore o altri diritti tutelati dalla normativa vigente;
- Navigare in siti con contenuti impropri quali pornografia, pedofilia, materiale blasfemo, molesto/osceno, razzismo, gioco d'azzardo, finalità ludiche, discriminatori per sesso, lingua, religione, razza, origine etnica; condizione di salute, opinione e appartenenza sindacale e/o politica.
- Scaricare immagini, file audio o musicali, file video o qualsiasi altro contenuto dal web che possa impegnare e degradare il sistema internet comunale, se non per i casi legati all'attività lavorativa;
- Utilizzare sistemi Peer to Peer, di file sharing, podcasting, webcasting e similari, collegarsi a siti che trasmettono programmi in streaming (radio o Tv via web), se non per motivi legati all'attività lavorativa.

Non è consentita l'attivazione sui P.C. di nessun collegamento ad internet se non espressamente autorizzato dagli Amministratori di sistema.

È da evitare ogni forma di registrazione a siti 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), se non per motivi legati all'attività lavorativa.

8) UTILIZZO DI TELEFONI FISSI, CELLULARI, PALMARI E SIMILI.

L'utilizzo di telefoni fissi, cellulari, palmari e simili che l'Amministrazione mette a disposizione è soggetto alle norme del presente disciplinare, come anche l'impiego disgiunto dell'apparato terminale o della scheda (o di altri sistemi hardware o software che, in futuro, dovessero anche parzialmente sostituirsi a quelli attualmente in uso).

Il telefono fisso, cellulare, palmare e simile che l'Amministrazione mette a disposizione deve essere utilizzato in modo strettamente pertinente allo svolgimento dell'attività lavorativa, secondo un utilizzo appropriato, efficiente, corretto e razionale.

Solo in caso di necessità e urgenza, i Lavoratori possono utilizzare tali beni per motivi non attinenti l'attività lavorativa e, comunque, non in modo ripetuto o per periodi di tempo prolungati. E' comunque preferibile, laddove possibile, che i Lavoratori utilizzino i propri telefoni.

In particolare, il telefono cellulare, palmare o simile deve essere custodito con diligenza e protetto da password. L'Amministrazione ha la facoltà di escludere esplicitamente alcuni di questi apparecchi dall'apposizione di password, quando non connessi, in alcun modo, ai sistemi informatici.

L'impiego di telefoni cellulari evoluti, palmari o di altri sistemi assimilabili (quelli che consentono l'accesso a internet, ovvero in grado di inviare messaggi di posta elettronica, di collegarsi via software con altri sistemi informatici, ecc.) è soggetto sia alle norme specifiche del presente capitolo che a quelle dell'intero Disciplinare, per quanto applicabili.

9) UTILIZZO DEI FAX

Il FAX che l'Amministrazione mette a disposizione deve essere utilizzato in modo strettamente pertinente allo svolgimento dell'attività lavorativa, secondo un utilizzo appropriato, efficiente, corretto e razionale.

10) UTILIZZO DI PARTICOLARI APPARATI

Per l'eventuale utilizzo di particolari apparati come macchine fotografiche o videocamere digitali, sistemi satellitari di rilevazione GPS, schede e sistemi di trasmissione dati wireless, ecc., verranno emanate norme apposite. In mancanza, si fa riferimento a quelle del presente Disciplinare, per quanto applicabili.

11) MONITORAGGI E GRADUALITA' DEI CONTROLLI

Qualsiasi forma di controllo venga effettuata, deve essere strettamente necessaria per il datore di lavoro in relazione a scopi determinati e per il perseguimento di finalità organizzative, produttive e di sicurezza, rispettando i principi di pertinenza e non eccedenza.

Il Comune di Castelfranco Veneto per ridurre il rischio derivante da minacce presenti nella rete internet (virus, spyware, adware, spam, phishing, ecc.) e per prevenire la navigazione in siti a contenuti impropri adotta opportune misure che possono così prevenire il più possibile eventuali controlli successivi sul lavoratore. Tali misure consistono in strumenti che filtrano i siti in base ad elenchi di siti non accessibili (black list) ed al contenuto della pagina e controllano il traffico telematico registrando temporaneamente su file log residenti sui server centralizzati gli accessi ad internet ed il traffico e-mail anomalo.

I log-file sono accessibili esclusivamente agli amministratori di sistema designati, al Titolare e al Responsabile del trattamento dei dati che li richiede e possono essere utilizzati esclusivamente per i motivi di seguito specificati.

Nel caso di eventi dannosi, di situazioni di pericolo o di anomalie riscontrate nell'utilizzo degli strumenti di lavoro che non siano stati impediti da preventivi accorgimenti tecnici, il Titolare o il Responsabile del trattamento dei dati può disporre dei controlli, di norma attraverso il personale del servizio Sistemi Informativi, inizialmente eseguendo un controllo preliminare su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree. Il controllo anonimo potrà concludersi con avvisi generalizzati alla singola area o settore in cui è stata rilevata l'anomalia, con l'invito ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. Solo successivamente e se l'utilizzo anomalo degli strumenti risulta reiterato, nonostante sia stato inoltrato l'esplicito invito agli utenti dell'area di attenersi ai compiti assegnati ed alle istruzioni impartite, si potrà procedere con controlli su base individuale.

In caso si giunga a controlli su base individuale e nominativa relativamente ad anomalie riscontrate sull'utilizzo della posta elettronica comunale, allorché non ci sia distinzione fra Posta Elettronica privata e professionale e la natura del messaggio non sia riconoscibile, l'Amministrazione presuppone che si tratti di posta elettronica professionale. Alla presenza di messaggi "Privati" o "Riservati" al datore di lavoro non è consentito prenderne visione. Alla presenza di fondati dubbi circa la natura professionale di un messaggio la questione deve essere chiarita con il Lavoratore.

Il personale del servizio Sistemi Informativi in caso di situazioni di pericolo per l'integrità dei dati e/o in genere per il corretto funzionamento del sistema informativo comunale, può effettuare il trattamento dei dati inizialmente in forma anonima e qualora risulti insufficiente alla risoluzione del problema con accesso totale, inoltrando l'eventuale prima segnalazione al Responsabile del trattamento in forma anonima senza l'indicazione di alcun nominativo di Lavoratori.

Va esclusa l'ammissibilità di controlli prolungati, costanti o indiscriminati.

I log-file relativi all'utilizzo di internet e della posta elettronica, i tabulati delle telefonate e dei fax sono conservati per il tempo necessario al perseguimento di finalità organizzative, produttive e di sicurezza. I log-file relativi agli accessi ad internet ed al traffico telematico sono periodicamente cancellati automaticamente dal sistema dopo 6 mesi.

Il prolungamento della conservazione dei log-file, può aver luogo solo nei seguenti casi:

- Per corrispondere ad eventuali richieste dell'autorità giudiziaria o della polizia giudiziaria;
- In caso di riscontro di anomalie, per esigenze tecniche o di sicurezza particolari, per il tempo strettamente necessario alla risoluzione delle anomalie riscontrate;
- All'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- Sino alla conclusione di procedimenti disciplinari e/o procedimenti penali per l'utilizzo anomalo degli strumenti di lavoro;

E' assolutamente vietato ai datori di lavori effettuare trattamenti di dati personali mediante sistemi hardware e software che mirano al controllo a distanza di lavoratori, svolti in particolare mediante:

- la lettura e la registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;
- la riproduzione e l'eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
- la lettura e la registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
- l'analisi occulta di computer affidati in uso;

12) SERVER FARM COMUNALE (C.E.D.)

La Server Farm comunale (C.E.D.) è sita al primo piano del Municipio. E' vietato l'accesso in quell'area senza il consenso del personale del servizio Sistemi Informativi, salvo che per operazioni di routine preautorizzate (ad es.: pulizie, nei soli limiti stabiliti per tale attività).

La gestione delle attrezzature all'interno della Server Farm comunale (C.E.D.) e dell'intera infrastruttura di trasmissione dei dati è riservata agli Amministratori di sistema designati.

13) OBBLIGATORIETÀ E SANZIONI

È fatto obbligo a tutti i Lavoratori di osservare le disposizioni portate a conoscenza con il presente Disciplinare.

Il mancato rispetto o la violazione delle regole contenute nel presente Regolamento è perseguibile con le azioni civili e penali previste dalla legge, nonché con i provvedimenti disciplinari previsti.

14) DISPOSIZIONI ULTERIORI

Le e-mail inviate e ricevute dai Rappresentanti Sindacali aventi titolo, per la parte qualificata e relativa all'attività sindacale, godono della tutela accordata alle e-mail di tipo "Privato" o "Riservato".

Il presente disciplinare può essere oggetto di revisione anche su eventuale proposta delle organizzazioni di rappresentanza dei Lavoratori o dei singoli Lavoratori.

In ogni caso il presente Disciplinare è soggetto a revisione con frequenza annuale.

Il presente disciplinare deve essere portato a conoscenza di tutti i lavoratori a cura dei Responsabili del trattamento designati dal Titolare del trattamento.

15) ESERCIZIO DEI DIRITTI

I lavoratori possono esercitare i diritti previsti dal D.Lgs. 196/2003 rivolgendosi al Titolare del Trattamento dei dati, Comune di Castelfranco Veneto, o rivolgendosi al Responsabile del Trattamento dei dati competente; per quanto attiene alla gestione del rapporto di lavoro rivolgendosi al dirigente di struttura.

Il Titolare del trattamento
Comune di Castelfranco Veneto

Castelfranco Veneto, lì _____

Il Responsabile del trattamento

Dott. _____

DICHIARAZIONE DI PRESA VISIONE DEL DOCUMENTO.

Il sottoscritto……..dichiara di aver preso visione e di aver ricevuto copia della circolare interna n.1 "Disciplinare per l'utilizzo degli strumenti elettronici, posta elettronica, internet, telefoni e fax del Comune" e si impegna al pieno rispetto di tali norme comportamentali.

In fede.

Luogo e data……..…….. Firma ……..

La presente comunicazione è redatta in due esemplari. Viene consegnata dal Responsabile del trattamento competente. Deve essere debitamente firmata ed una copia viene restituita al Responsabile del trattamento ; una copia rimane all'incaricato.