ALLEGATO A)

# COMUNE DI TEOLO

## *Regolamento per l' utilizzo della Posta elettronica e di Internet nel sistema informatico del Comune di Teolo*

## Articolo 1 - Finalità del regolamento

1. Il regolamento stabilisce le modalità di utilizzo delle risorse informatiche del Comune al fine di un corretto utilizzo delle stesse, nonché le modalità con le quali possono essere effettuati controlli.
2. Al fine di tutelare i reciproci diritti e doveri dei lavoratori e del datore di lavoro si definiscono in particolare:
- le modalità per l'utilizzo e l'accesso al servizio internet e di posta elettronica, da parte dei dipendenti comunali e di tutti gli altri soggetti che a vario titolo prestano servizio o attività per conto e nelle strutture del Comune;
- il diritto dell'Amministrazione di monitorare che non si verifichino usi impropri;
- il diritto del lavoratore ad una sfera di riservatezza anche nelle relazioni lavorative.
3. Le prescrizioni del presente regolamento si aggiungono e integrano le norme già previste dal contratto collettivo nazionale di lavoro, nonché dalla normativa in materia di protezione dei dati personali contenuta nel D.Lgs. 196/2003.

## Articolo 2 - Utilizzo dei sistemi informatici

1. I dipendenti e gli altri soggetti autorizzati all'utilizzo dei sistemi informatici comunali rispettano le seguenti indicazioni:
- le apparecchiature informatiche (personal computer, stampanti, periferiche in genere) sono strumenti di lavoro affidati al dipendente e vanno custoditi in modo appropriato nonché utilizzati solo per fini istituzionali;
- non è consentito modificare le configurazioni impostate sulla propria postazione di lavoro;
- tutti gli utilizzatori sono tenuti al rispetto delle leggi in materia di tutela della proprietà intellettuale e non possono, senza autorizzazione dell'amministrazione di sistema, installare sulle apparecchiature affidate hardware o software, nè duplicare o utilizzare software che non sia stato preinstallato, installato o comunque fornito dal Comune;
- non è consentito utilizzare strumenti software e/o hardware atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
- salvo quanto previsto all'articolo 4, comma 4, l'uso della postazione di lavoro e delle relative periferiche è finalizzato all'esclusivo svolgimento dell'attività lavorativa o di servizio;
- non è ammesso l'uso in genere delle risorse informatiche per l'archiviazione di documenti personali (quali ad esempio documenti, programmi, immagini, audio, video, archivi in genere). Casi particolari devono essere espressamente autorizzati dall'amministratore di sistema.
- Salva debita autorizzazione non è consentita la duplicazione, il trasferimento o la diffusione, all'esterno del sistema informatico di banche dati o di dati interni personali nè attraverso supporti hardware personali (ad esempio floppy disk, cd, dvd, pen drive, notebook, dischi esterni), nè con altri strumenti telematici (quali ad esempio la posta elettronica o siti internet pear to pear).

2. Per l'accesso alle postazioni di lavoro informatiche ci si deve attenere alle seguenti disposizioni:
- utilizzare direttamente le credenziali personali (nome utente e password) assegnate per accedere alle procedure informatiche e non comunicarle a nessuno;

- non consentire a terzi l'accesso alla apparecchiatura informatica con le proprie credenziali e non lasciare incustodita ed accessibile la propria postazione una volta connessa al sistema; in ogni caso il personal computer deve essere spento al termine del servizio giornaliero.
- non utilizzare credenziali di altri utenti, nemmeno se fornite volontariamente o di cui si ha casualmente conoscenza;
- non cedere a terzi, una volta superata la fase di autenticazione, l'uso della propria stazione, in particolar modo per quanto riguarda l'accesso a internet e ai servizi di posta elettronica;
- è fatto obbligo di adottare le necessarie cautele per assicurare la segretezza delle credenziali assegnate. La perdita o la conoscenza dell'utilizzo da parte di altri delle proprie credenziali deve essere comunicata all'amministratore di sistema il quale provvederà al rilascio di nuove e sostitutive modalità di autenticazione al sistema informatico.

3. In caso di assenza o impedimento del dipendente, qualora si renda indispensabile e indifferibile intervenire nella relativa postazione, per necessità di operatività e di sicurezza del sistema o per ragioni che compromettano gravemente il buon andamento dell'amministrazione, l'amministratore di sistema procede a rigenerare una nuova password, diversa da quella in uso al dipendente assente, che verrà utilizzata per l'accesso. Dell'eventuale accesso così effettuato, verrà data comunicazione al dipendente e si provvederà, al rientro di quest'ultimo, ad assegnare una nuova parola chiave. Di tale operazione è conservato verbale.

## Articolo 3 - Utilizzo di Internet

1. Non è consentito accedere a siti non attinenti lo svolgimento di compiti istituzionali.
2. Non è consentita l'effettuazione di ogni genere di transazione finanziaria, comprese le operazioni di remote banking, acquisti on line e simili, salvo i casi autorizzati per ragioni di servizio, nel rispetto delle vigenti procedure di acquisto.
3. Non è consentito lo scarico di software gratuiti (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato.
4. Non è consentito lo scarico di file musicali, film, multimediali in genere se non espressamente autorizzato o pertinente l'attività lavorativa. Non è consentito altresì detenere nelle unità di rete o nei dischi della postazione di lavoro documenti del genere indicato anche se non provenienti da internet.
5. E' vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa né è permessa la partecipazione a forum, per motivi non connessi all'attività istituzionale, né l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guestbook (anche utilizzando pseudonimi) o spazi virtuali.
6. E' consentita la navigazione solo in siti correlati con le attività, i procedimenti e le relazioni istituzionali (ad esempio siti delle istituzioni comunitarie, delle amministrazioni centrali e periferiche dello stato, sanità, regioni, province, comuni, unioni di comuni, comunità locali, autorità giudiziaria, enti previdenziali e assistenziali, fornitori, provider, enti economici, centri servizi, terzo settore, siti che mettono a disposizioni informazioni, banche dati e forum di interesse comunale...)

## Articolo 4 - Disposizioni relative all'utilizzo del sistema di Posta Elettronica

1. Non è consentito utilizzare la posta elettronica (interna ed esterna) per motivi non attinenti

allo svolgimento delle mansioni assegnate.
2. Non è consentito inviare, memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
3. Le caselle di posta elettronica assegnate alle varie posizioni di lavoro sono da considerarsi a tutti gli effetti caselle di posta elettronica istituzionali.
4. Al personale è consentito l'accesso a proprie caselle di posta elettronica – cioè caselle di posta elettronica diverse da quelle assegnate dal Comune - per ragioni personali, ricorrendo a sistemi di webmail. Ciò al di fuori dell'orario di lavoro. In via eccezionale è consentito, un uso moderato della casella di posta elettronica personale anche nel tempo di lavoro.
5. Possono essere temporaneamente memorizzate le tracce delle comunicazioni in registri denominati file di log, al fine di garantire una corretta gestione e il controllo per evitare comunicazioni indesiderate, per sottoporre gli allegati a controllo antivirus e per la verifica della disponibilità e funzionalità del sistema hardware e software di gestione della posta elettronica. Gli accessi alle procedure di controllo di diagnosi di eventuali anomalie sono esclusivamente di natura interna. Dette registrazioni sono conservate solo per il tempo necessario al raggiungimento del buon fine delle comunicazioni e sono regolarmente eliminate o sovrascritte.
6. Il Comune si riserva la facoltà di effettuare controlli in conformità alla legge, anche saltuari o occasionali, qualora si verifichino condizioni di attacco informatico, di malfunzionamenti segnalati, di necessità di aumentare i livelli delle misure di sicurezza, di abusi nell'utilizzo.
7. Qualora si verifichino le condizioni citate saranno emessi dei comunicati collettivi o individuali.
8. Si raccomanda l'attivazione di apposite funzionalità di sistema, di agevole utilizzo, che consentano di inviare automaticamente, in caso di assenze (ad es. per ferie o attività di lavoro fuori sede), messaggi di risposta contenenti le "coordinate" (anche elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto della struttura.
9. 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 della casella assegnata al dipendente, ogni dipendente ha facoltà di comunicare al proprio responsabile del servizio il nominativo di un altro dipendente delegato e fiduciario, che possa procedere a verificare il contenuto di messaggi e a inoltrare al responsabile del servizio quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Se si verifica la condizione di accesso alla casella di posta elettronica assegnata al dipendente, da parte del delegato o fiduciario, il responsabile del servizio provvede a redigere apposito verbale ed a informare il dipendente interessato alla prima occasione utile.
10. E' vietato inviare catene telematiche e di attivare gli allegati di eventuali messaggi di tale tipo, in particolare se contenenti file con estensione ".exe".
11. La casella di posta elettronica deve essere mantenuta in ordine, cancellando documenti inutili, in particolare se contenenti allegati ingombranti.

## Articolo 5 - Conservazione

1. I sistemi software sono programmati e configurati in modo da cancellare periodicamente ed automaticamente, attraverso procedure di sovraregistrazione, i registri delle attività generati dai programmi informatici di gestione dei sistemi di posta elettronica e dei programmi informatici che permettono l'accesso ad internet.
2. I tempi di conservazione dei registri di attività sono determinati in un tempo massimo di sei mesi, dopo i quali, detti registri vengono soprascritti. L'accesso alle registrazioni ed eventuali motivate deroghe ai tempi sopra indicati, hanno luogo solo in relazione:

- ad esigenze tecniche o di sicurezza;
- all'adempimento di altre normative imposte dal Garante in ordine alle attività dell'Amministratore di sistema;
- ad eventuali richieste dell'autorità giudiziaria;
- alla necessità di effettuare dei controlli ai sensi del successivo punto 6.

## Articolo 6 - Controlli

1. I controlli sono obbligatori per legge in adempimento degli articoli da 31 a 35 e del disciplinare tecnico in materia di misure minime di sicurezza Allegato B) al D.Lgs. 196/2003 al fine di attuare le procedure di protezione dei dati personali contro il rischio di intrusione di cui all'art. 615 ter del codice penale e dell'azione di programmi di cui all'art. 615-quinquies del codice penale. Il Comune è altresì tenuto, in quanto datore di lavoro, ad assicurare la funzionalità ed il corretto impiego degli strumenti ICT da parte dei propri dipendenti, adottando le misure necessarie a garantire la sicurezza, la disponibilità e l'integrità dei sistemi informativi.
2. Nell'effettuare detti controlli sull'uso degli strumenti elettronici viene accuratamente evitata qualsiasi interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata. Detti controllo rispettano i principi di pertinenza e non eccedenza.
3. Nel caso in cui un evento dannoso o una situazione di pericolo non siano stati impediti con preventivi accorgimenti tecnici, la direzione può adottare eventuali misure che consentano la verifica di comportamenti anomali.
4. Il controllo è preliminare su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree. Non è prevista e quindi esclusa, la condizione di controlli prolungati, costanti o indiscriminati. Il controllo anonimo può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. L'avviso può essere successivamente circoscritto a specifiche aree o anche a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia o il mancato rispetto di direttive poste dall'amministratore di sistema.

## Articolo 7 – Mancata osservanza delle disposizioni regolamentari

1. L'utente è responsabile di qualsiasi danno arrecato in dipendenza della mancata osservanza di quanto previsto dal presente regolamento. L'utente può essere chiamato a rispondere civilmente, oltre che per i propri fatti illeciti, anche per quelli commessi da chiunque utilizzi il suo codice identificativo e/o password, con particolare riferimento all'immissione in rete di contenuti non ammessi o in genere in contrasto con la legislazione italiana.
2. La violazione delle presenti disposizioni può comportare infine l'applicazione delle sanzioni disciplinari previste dal vigente contratto collettivo nazionale di lavoro, rimanendo ferma ogni ulteriore forma di responsabilità penale.

## Articolo 8 - Misure di sicurezza adottate

1. Le misure di sicurezza che sono state adottate al fine di assicurare il più alto livello di disponibilità, integrità e riservatezza del sistema di posta elettronica e del sistema di accesso alla rete internet sono le seguenti:

- attivazione di apparati che provvedono alla ricezione e invio di posta elettronica contrastando messaggi indesiderati e applicando livelli commisurati di protezione dalle vulnerabilità conosciute sia sui messaggi che sugli allegati;
- attivazione di apparati che tendono a restringere il campo di consultazione ai soli web-site che sono stati definiti come "pertinenti" ed "utili". Ogni utente che dia vita ad una sessione di browsing internet, sarà soggetto al vaglio un servizio di web-blocking, il quale comunicherà in risposta l'assenso o il diniego all'apertura della specifica pagina web.

## Articolo 9 - Disposizioni finali

1. Il presente regolamento costituisce estensione e integrazione delle informative dovute ai sensi dell'art. 13 del D.Lgs. 196/2003.
2. Il Comune nella sua azione costante - anche in relazione alle conoscenze acquisite in base al progresso tecnico - tesa al miglioramento delle misure di sicurezza al fine di ridurre al minimo il rischio di distruzione o perdita anche accidentale dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme, si riserva di emanare ulteriori disciplinari interni, con i quali saranno dettate o aggiornate le regole generali di comportamento nell'uso della strumentazione elettronica.
3. Il presente regolamento è pubblicato nel sito internet del Comune, consegnato ad ogni dipendente in servizio, nonchè ad ogni altro soggetto autorizzato all'accesso al sistema informatico comunale attraverso postazioni in rete e non.