Regolamento per l'utilizzo della rete e dei servizi informatici

Articolo 1
OGGETTO E AMBITO DI APPLICAZIONE

Il presente regolamento disciplina le modalità di accesso e di uso della rete informatica e telematica del Comune di Camaiore, connessa alla rete Internet, e dei servizi che, tramite la stessa rete, è possibile ricevere e offrire.

Articolo 2
PRINCIPI GENERALI – DIRITTI E RESPONSABILITÀ

1. Il Comune di Camaiore promuove l'utilizzo della rete dei servizi informatici e telematici (*la rete*, nel seguito) quale strumento utile per perseguire le proprie finalità e individua nell'Ufficio Sistemi Informativi il servizio interno cui affidarne, da un punto di vista tecnico, la gestione, la manutenzione e l'evoluzione.

2. I soggetti autorizzati come da Art. 5 ad accedere alla rete (*gli utenti* della rete, nel seguito) utilizzano le risorse e i servizi della rete nel rispetto dell'integrità dei sistemi, in osservanza delle leggi, norme e obblighi contrattuali.

3. Ogni utente è responsabile del diligente mantenimento delle attrezzature informatiche utilizzate, al fine di preservarne funzionalita' ed efficienza. In particolare deve anche provvedere allo spegnimento delle attrezzature in uso, al termine del suo orario di lavoro, se non sono necessarie ad altri utenti.

4. Ogni utente e' tenuto ad operare ponendo attenzione al contenimento del consumo di materiali informatici quali supporti per la memorizzazione dei dati (floppy disc, CD, DVD, etc.) e cartucce e toner di stampanti, privilegiando l'uso e la diffusione del documento elettronico rispetto a quello cartaceo.

5. Gli utenti, consapevoli delle potenzialità offerte dagli strumenti informatici e telematici, si impegnano ad agire con responsabilità e a non commettere abusi aderendo ad un principio di autodisciplina. Con il termine di abuso si intende qualsiasi violazione del presente regolamento e di altre norme civili, penali e amministrative che disciplinano le attivita' e i servizi svolti sulla rete e di condotta personale.

6. Ogni postazione di lavoro informatizzata viene assegnata completa dei dispositivi (*hardware*) e dei programmi di base e degli applicativi specifici (*software*), necessari per svolgere le funzioni di base richieste dall'attivita' dell'ufficio, d'intesa con il Dirigente/Responsabile del Servizio interessato, e compatibilmente con le licenze d'uso disponibili e le risorse economiche e strumentali dell'Ente. E' pertanto vietato agli utenti modificarne la configurazione di base e installare, modificare, rimuovere o spostare qualsiasi attrezzatura o dispositivo hardware e installare, rimuovere o alterare qualsiasi software di qualunque tipo e origine.

7. Tutte le richieste di installazioni, realizzazioni e ristrutturazioni hardware e software devono essere valutate congiuntamente dal Dirigente/Responsabile del Servizio interessato e dalla UO Sistemi Informativi, cui spetta la verifica tecnica della compatibilita' degli strumenti richiesti con l'infrastruttura di rete e la normativa vigente, con particolare riferimento alla sicurezza delle banche dati dell'Ente. In particolare, non possono essere effettuate realizzazioni, ristrutturazioni, acquisizioni e installazioni di attrezzature e/o componenti hardware e/o software senza preventiva valutazione e visto tecnico della UO Sistemi Informativi. Nel caso in cui gli strumenti proposti non possano, per ragioni tecniche, essere installati, saranno individuate, ove possibile e nei limiti della tecnologia, soluzioni alternative, tecnicamente fattibili, d'intesa tra la UO Sistemi Informativi e il servizio interessato. Gli strumenti e i sistemi hardware/software tecnicamente utilizzabili saranno resi disponibili dalla UO Sistemi Informativi (o da personale tecnico da questa esplicitamente autorizzato), compatibilmente con le licenze d'uso disponibili e le risorse economiche e strumentali dell'Ente. I software acquistati e le relative licenze devono essere conservati presso la UO Sistemi Informativi, cosi' da consentire le operazioni di verifica della disponibilita' di licenze e l'eventuale installazione.

8. Ogni utente e' responsabile della conservazione dei dati e dei documenti elettronici di qualsiasi tipo, formato e natura che utilizza, sia sulla propria postazione di lavoro informatizzata che su altre, se, per esigenze d'ufficio, e' in regime di condivisione di risorse. Per questo motivo ogni utente è tenuto ad effettuare la copia di questi dati e documenti secondo le modalita' del servizio "Area Salvataggio Documenti Informatici", attivato il 18/01/2003 con Prot. N. 51732/2003. In caso di guasto, malfunzionamento o sostituzione di una postazione di lavoro informatizzata, nonche' di cancellazioni o modifiche accidentali, potranno essere recuperati soltanto i documenti preventivamente salvati tramite questo servizio, la cui continuita' ed affidabilita' e' garantita, per quanto possibile e compatibilmente con gli standard tecnologici, dalla UO Sistemi Informativi. Qualsiasi documento non preventivamente salvato in quest'area a cura dell'utente e in maniera autonoma, non potra' in alcun caso essere recuperato, con possibile danno per l'Ente.

Articolo 3
ABUSI E ATTIVITÀ VIETATE

E' vietato ogni tipo di abuso, secondo quanto definito all'Art. 2 del presente regolamento. In particolare è vietato:

1. usare la rete in modo difforme da quanto previsto dalle leggi penali, civili e amministrative e da quanto previsto dal presente regolamento;
2. utilizzare la rete per scopi personali o incompatibili o non inerenti con l'attività istituzionale del Comune di Camaiore;
3. utilizzare una credenziale di autenticazione personale (nome utente e/o password o smart-card) a cui non si è autorizzati;
4. cedere a terzi credenziali di autenticazione personali (nome utente e/o password o smart-card) di accesso ai sistemi informatici;

5. conseguire l'accesso non autorizzato a risorse di rete interne o esterne alla rete del Comune di Camaiore;
6. violare la riservatezza di altri utenti o di terzi;
7. agire deliberatamente con attività che influenzino negativamente la regolare operatività della rete e ne restringano l'utilizzabilità e le prestazioni per altri utenti (es.: uso di programmi di file-sharing e/o p2p, etc.);
8. effettuare o permettere ad altri trasferimenti non autorizzati di informazioni (software, licenze, dati, etc.);
9. utilizzare software o servizi di cui non si disponga della licenza d'uso;
10. installare o eseguire deliberatamente o diffondere su qualunque computer e sulla rete, programmi destinati a danneggiare, sovraccaricare i sistemi o la rete o carpire informazioni e dati (es.: virus, dialer, etc.)
11. cancellare, disinstallare, copiare, spostare o asportare programmi e componenti hardware/software o licenze d'uso;
12. installare componenti e/o programmi software senza l'autorizzazione della UO Sistemi Informativi (es.: stampanti, tastiere, lettori MP3, software di terze parti, etc.)
13. utilizzare caselle di posta elettronica e servizi "Web-Mail" non direttamente riconducibili al Comune di Camaiore (es.: caselle e/o servizi quali yahoo, hotmail, tiscali, etc.)
14. utilizzare la posta elettronica e i servizi Internet inviando e/o ricevendo materiale che violi le leggi;
15. collegarsi a siti e/o servizi Internet non inerenti l'attivita' dell'ufficio e/o dell'Ente;
16. aprire o salvare in qualsiasi formato e su qualsiasi supporto messaggi di posta elettronica, il cui oggetto sia marcato con la dicitura "VIRUS" o altra dicitura simile.
17. accedere direttamente ad Internet e/o a reti e servizi esterni con modem collegato alla propria postazione informatizzata, se non espressamente autorizzati dalla UO Sistemi Informativi e per particolari motivi tecnici;
18. utilizzare sistemi o servizi personali di messaggistica (instant messaging), di chat, di telefonia su Internet (VOIP) o simili;
19. monitorare o utilizzare qualunque tipo di servizio e sistema informatico o elettronico per controllare le attività degli utenti; leggere, copiare o cancellare file e software di altri utenti, senza averne l'autorizzazione;
20. usare l'anonimato o servirsi di risorse che consentano di restare anonimi sulla rete;
21. modificare password di accesso ai sistemi e ai servizi;
22. abbandonare la postazione informatizzata, lasciandola incustodita e accessibile, ovvero, se accessibile, senza aver verificato l'attivazione del servizio di salvaschermo protetto da password.

Articolo 4
ATTIVITÀ CONSENTITE

1. Agli utenti sono consentite tutte le attivita' non espressamente vietate dalla legge, dal presente regolamento o da altri provvedimenti dell'Ente.

2. La UO Sistemi Informativi, per il corretto svolgimento dei suoi compiti istituzionali e per finalita' di ricerca e sviluppo necessarie alla crescita

dell'infrastruttura di rete e dei servizi informatici dell'Ente, puo' derogare dai divieti del presente regolamento, fermo restando il rispetto degli obblighi normativi.

In particolare, alla UO Sistemi Informativi e' anche consentito:

a) Monitorare o utilizzare qualunque tipo di servizio e sistema informatico o elettronico per controllare il corretto utilizzo delle risorse di rete (postazioni informatizzate e componenti software), per copiare o rimuovere file e software, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori. In particolare e' consentito alla UO Sistemi Informativi, al fine di garantire un efficiente livello di servizio, l'utilizzo di servizi e sistemi di "Teleassistenza", che consentono al personale della UO Sistemi Informativi, o a personale tecnico di terze parti da questa esplicitamente autorizzato, di accedere da remoto alle postazioni informatizzate. In questo caso l'operatore alla postazione informatizzata sottoposta a Teleassistenza sara' avvisato, o telefonicamente o tramite altre forme ritenute idonee, al momento dell'intervento stesso;
b) Monitorare o utilizzare qualunque tipo di servizio e sistema informatico o elettronico per supervisionare la navigazione Internet e il traffico di posta elettronica, sia per esigenze statistiche che di controllo della spesa e dell'utilizzo dei servizi. L'attivita' di monitoraggio consiste esclusivamente nel tenere traccia, per ogni postazione di lavoro informatizzata, del nome della pagina Internet visitata, e degli indirizzi di destinazione e provenienza dei messaggi di posta elettronica. Il contenuto delle pagine Internet visitate e dei messaggi di posta elettronica entranti/uscenti non sono in alcun modo soggetti a monitoraggio, in accordo al principio di autodisciplina espresso dall'Art. 2.
c) Adottare le necessarie misure tecniche preventive e/o a posteriori per garantire un adeguato livello di sicurezza della rete, incluso il blocco temporaneo o definitivo della navigazione su siti Internet e/o su domini di posta elettronica. In accordo al principio di autodisciplina espresso dall'Art. 2, e nel rispetto delle attivita' vietate all'Art.3, la fruizione di Internet e della Posta Elettronica risulta libera, e ogni utente e' responsabile della navigazione e dello scambio di messaggi dalla postazione di lavoro assegnatagli. Alla UO Sistemi Informativi e' demandato, compatibilmente con quanto la tecnologia consente, di attivare i meccanismi idonei ad interdire i siti Internet il cui accesso comporta palesemente la violazione degli Artt. 2 e 3. Qualsiasi altro sito sara' interdetto solo su richiesta esplicita di Dirigenti/Responsabili di Servizio. In caso di rischi riconosciuti per la sicurezza del sistema informativo dell'Ente (diffusione di virus, etc etc), la UO Sistemi Informativi, su sua iniziativa, potra' chiudere qualsiasi sito, ma soltanto temporaneamente, per la sola durata dell'emergenza, e comunicando tempestivamente a tutti gli uffici la durata presunta del blocco.

Articolo 5
SOGGETTI CHE POSSONO AVERE ACCESSO ALLA RETE E AI SERVIZI

1. Hanno diritto ad accedere alla rete del Comune di Camaiore:

a) i dipendenti, se autorizzati dal Dirigente/Responsabile del Servizio cui sono assegnati;
b) i collaboratori esterni impegnati nelle attività istituzionali per il periodo di collaborazione, se autorizzati dal Dirigente/Responsabile del Servizio interessato;
c) il Sindaco e i componenti l'Amministrazione (Assessori, Presidente del Consiglio, Consiglieri Comunali, Presidenti e Consiglieri di Circoscrizione), per la durata del mandato o delega, se autorizzati dal Sindaco e per le sole attivita' istituzionali;
d) il personale tecnico di terze parti per motivi di manutenzione ordinaria/straordinaria e limitatamente alle applicazioni, ai servizi e all'infrastruttura di competenza per il periodo necessario all'intervento, se espressamente autorizzato dalla UO Sistemi Informativi;

2. L'accesso alla rete è assicurato compatibilmente con le potenzialità delle attrezzature e nei limiti imposti dalla tecnologia, tramite il rilascio, ai soggetti autorizzati, di credenziali di autenticazione (coppie utente/password o simili) da parte della UO Sistemi Informativi.

3. Con l'obiettivo di garantire un adeguato livello di sicurezza e il miglior funzionamento delle risorse di rete disponibili, la UO Sistemi Informativi puo':
   a) regolamentare l'accesso alla rete di determinate categorie di utenti, quando questo è richiesto da ragioni tecniche;
   b) adottare apposite disposizioni di carattere operativo che gli utenti si impegnano ad osservare.

4. L'accesso ai servizi e ai programmi applicativi è consentito solo agli utenti che hanno accesso alla rete e che, per motivi di servizio, ne devono fare uso.

5. Le password di accesso ai sistemi informatici (software applicativi e banche dati) vengono rilasciate e revocate esclusivamente dalla UO Sistemi Informativi solo e soltanto su richiesta dei Dirigenti/Responsabili dei Servizi, cui quei sistemi e/o quelle banche dati fanno riferimento.

6. Ad ogni variazione del personale assegnato ad un ufficio, i Dirigenti/Responsabili dei Servizi coinvolti, ciascuno per la propria competenza, devono comunicare alla UO Sistemi Informativi il nominativo del personale da variare e i servizi informatici per i quali assegnare o revocare la credenziale di accesso (password).

7. Ad ogni variazione delle mansioni del personale assegnato ad un ufficio, il Dirigente/Responsabile del Servizio deve comunicare alla UO Sistemi Informativi il nominativo del personale da variare e i servizi informatici per i quali assegnare o revocare la credenziale di accesso (password).

8. I soggetti che accedono alla rete e ai servizi informatici devono richiedere alla UO Sistemi Informativi la sostituzione delle proprie credenziali di accesso nel caso in cui sia stata compromessa la loro riservatezza e almeno una volta ogni sei mesi, salvo diverse disposizioni di legge.

Articolo 6
MODALITÀ DI ACCESSO ALLA RETE E AI SERVIZI

1. Qualsiasi accesso alla rete e ai servizi informatici viene associato ad una persona fisica o ad un'entita' giuridica, cui sono attribuite le attività svolte utilizzando le credenziali di autenticazione assegnategli. Tutte le attivita' svolte sono registrate elettronicamente e soggette a supervisione per esigenze statistiche, di controllo della spesa e a garanzia del livello di sicurezza della rete.

2. L'utente che ottiene l'accesso alla rete e ai servizi si impegna ad osservare il presente regolamento e le altre norme disciplinanti le attività e i servizi che si svolgono via rete e si impegna a non commettere abusi e a non violare i diritti degli altri utenti e dei terzi, assumendosi la totale responsabilità delle attività svolte.

3. Ad ogni utente autorizzato come da Art. 5 del presente regolamento sono assegnate e comunicate dalla UO Sistemi Informativi:
   a) una password di accensione della postazione informatizzata normalmente utilizzata come da indicazione del Dirigente/Responsabile del Servizio interessato; tale password, su richiesta, puo' essere comunicata al Responsabile dell'Ufficio per consentire l'accesso alla postazione da parte del personale dell'ufficio stesso.
   b) le credenziali (nome utente e password) per l'accesso alla rete informatica da qualsiasi postazione informatizzata. Tali credenziali sono strettamente personali, in quanto identificano in maniera univoca chi accede alla rete e ai servizi dell'Ente, incluse le banche dati. Ciascun utente deve adottare le necessarie cautele per assicurarne la segretezza e la diligente custodia. Il Responsabile dell'Ufficio puo' custodire o richiedere una copia di queste credenziali, da usare nel caso di assenza o impedimento che renda indispensabile e indifferibile intervenire, accedendo con quelle credenziali, per esclusiva necessità operativa. In tal caso, immediatamente superata la necessità, deve essere richiesto all'ufficio Sistemi Informativi la sostituzione delle credenziali divulgate.

Articolo 7
SANZIONI

In caso di abuso, a seconda della gravità del medesimo, e fatte salve ulteriori conseguenze di natura penale, civile e amministrativa, possono essere comminate le sanzioni disciplinari previste dalla normativa vigente in materia e dai regolamenti del Comune di Camaiore.