DISCIPLINARE PER L'UTILIZZO DEL SISTEMA INFORMATIVO DEL COMUNE DI REFRONTOLO

TITOLO I

MISURE GENERALI PER L'UTILIZZO DEL SISTEMA INFORMATIVO

ART. 1 - OGGETTO

1. Il presente disciplinare regolamenta le modalità di accesso e di uso della rete informatica e telematica del Comune di Refrontolo e dei servizi che, tramite la rete stessa, è possibile ricevere o offrire.

ART. 2 - PRINCIPI GENERALI - DIRITTI E RESPONSABILITÀ

1. Il Comune di Refrontolo promuove l'utilizzo della rete quale strumento utile per perseguire le proprie finalità. Gli utenti manifestano liberamente il proprio pensiero nel rispetto dei diritti degli altri utenti e di terzi, nel rispetto dell'integrità dei sistemi e delle relative risorse fisiche, in osservanza delle leggi, norme e obblighi contrattuali.
Consapevoli delle potenzialità offerte dagli strumenti informatici e telematici, gli utenti si impegnano ad agire con responsabilità e a non commettere abusi aderendo a un principio di autodisciplina.
2. Le dotazioni informatiche (PC, notebook, tablet, smartphone, ecc.) affidate al Dipendente sono uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa non è consentito, fatto salvo i casi normati in questo disciplinare, in quanto può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.
3. Le dotazioni informatiche vengono consegnate complete di quanto necessario per svolgere le proprie funzioni, pertanto è vietato modificarne la configurazione.
I software installati sono quelli richiesti dalle specifiche attività lavorative dell'operatore. E' pertanto proibito installare autonomamente qualsiasi programma, senza l'autorizzazione del Responsabile del sistema informatico.
4. Solo i file che si trovano nella cartella di sistema “Documenti” del proprio PC sono soggetti a backup giornalieri. Altri file (es: quelli salvati sul proprio desktop) non lo sono.
5. Qualsiasi dotazione informatica deve essere spenta alla fine della giornata lavorativa o in caso di assenze prolungate, fatto salvo i casi in cui, dietro comunicazione degli addetti del sistema informatico, vada lasciata accesa per eseguire manutenzioni o programmi per la rilevazione di virus o codici malevoli. E’ importante non lasciare la sessione aperta quando ci si allontana dal PC o dal notebook. In questo caso è necessario bloccare la sessione o fare il logout.
6. 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 deve essere salvato.
7. Il Titolare della gestione dei dati può in qualunque momento, anche attraverso suoi incaricati, procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosa per la sicurezza, da qualsiasi dotazione informatica.
8. Costituisce buona regola la periodica cancellazione dei file obsoleti e/o inutili e delle scansioni effettuate e salvate nella cartella condivisa. Particolare attenzione deve essere prestata alla duplicazione dei dati. E' infatti assolutamente da evitare un'archiviazione ridondante.
9. Tutti i supporti magnetici e rimovibili riutilizzabili (Hard Disk esterni USB, Memory card, chiavette USB, ecc.) contenenti dati personali devono essere trattati con particolare cautela, onde evitare che il loro contenuto possa essere recuperato. Prima di memorizzare dei dati personali su

supporti removibili che verranno successivamente utilizzati esternamente all'Ente, è necessario accertarsi che questi non contengano altri dati.
10. I supporti removibili contenenti dati sensibili devono essere custoditi in archivi chiusi a chiave.
11. I dati sensibili non più utilizzati memorizzati su supporti removibili devono essere resi non leggibili e tecnicamente non ricostruibili attraverso un'opportuna procedura di cancellazione.

ART. 3 - UTILIZZO DI DOTAZIONI INFORMATICHE PORTATILI

1. L'utente è responsabile delle dotazioni informatiche portatili, quali notebook, tablet, smartphone, cellulari, ecc., assegnategli e deve custodirle con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
2. Alle dotazioni informatiche portatili si applicano le regole di utilizzo previste per i normali PC connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.
3. Alle dotazioni informatiche portatili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi in un luogo protetto.

ART. 4 - UTILIZZO DI MULTIFUNZIONI E STAMPANTI DI RETE

1. E' cura del personale effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti (soprattutto per le stampanti di rete siti in luoghi facilmente accessibili al pubblico).

ART. 5 - ABUSI E ATTIVITÀ VIETATE

1. Si intende con abuso qualsiasi violazione del presente disciplinare e di altre norme civili, penali e amministrative che disciplinano le attività e i servizi svolti sulla rete e di condotta personale.
2. E' vietato ogni tipo di abuso. In particolare è vietato:

- usare la rete in modo difforme da quanto previsto dal presente disciplinare.
- usare la rete in modo difforme da quanto previsto dalle leggi penali, civili e amministrative.
- utilizzare la rete aziendale e quella internet per scopi incompatibili con l'attività istituzionale del Comune di Refrontolo, fermi restando i casi successivamente disciplinati.
- utilizzare codici di accesso non propri.
- cedere a terzi i propri codici di accesso al sistema.
- conseguire l'accesso non autorizzato a risorse di rete interne o esterne.
- agire con attività che influenzino negativamente la regolare operatività della rete e ne restringano l'utilizzabilità e le prestazioni per altri utenti.
- fare o permettere ad altri trasferimenti non autorizzati di informazioni (software, basi dati, ecc.)
- installare, eseguire o diffondere software non autorizzati su qualunque dotazione informatica e sulla rete, programmi destinati a danneggiare o sovraccaricare i sistemi o la rete; come a titolo esemplificativo virus, cavalli di troia, programmi di file sharing, ecc.
- cancellare, disinstallare, copiare programmi software per scopi personali.
- rimuovere, danneggiare o asportare componenti hardware.
- utilizzare la posta elettronica inviando e ricevendo materiale che violi le leggi.
- leggere, copiare o cancellare files e software di altri utenti, senza averne l'autorizzazione esplicita.
- usare l'anonimato o servirsi di risorse che consentano di restare anonimi.
- Abbandonare il posto di lavoro lasciando la sessione aperta.

ART. 6 - ATTIVITÀ CONSENTITE ALL'AMMINISTRATORE DI SISTEMA

1. 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, è consentito all'Amministratore di sistema:

- monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare il corretto utilizzo delle risorse di rete (sia intranet che internet), delle dotazioni informatiche e degli applicativi;
- creare e reimpostare password nel caso di emergenza;
- Rimuovere e installare programmi software e componenti hardware.

ART. 7 - SOGGETTI CHE POSSONO AVERE ACCESSO AL SISTEMA INFORMATICO

1. Hanno la possibilità di accedere al sistema informatico del Comune di Refrontolo il Segretario comunale, i dipendenti, le ditte fornitrici di software per motivi di manutenzione e limitatamente alle applicazioni di loro competenza, i collaboratori a qualsiasi titolo impegnati nelle attività istituzionali limitatamente al periodo di collaborazione.
2. Per fini istituzionali hanno la possibilità di accedere al sistema informatico il Sindaco, nonché gli Assessori e gli altri amministratori, a ciò autorizzati dal Sindaco medesimo.
3. L'accesso alla rete è assicurato compatibilmente con le potenzialità delle attrezzature.
4. L'Amministratore di sistema può regolamentare con policy l'accesso alla rete di determinate categorie di utenti, quando questo è richiesto per ragioni tecniche.
6. L'accesso agli applicativi è consentito agli utenti che, per motivi di servizio, ne devono fare uso.

ART. 8 - MODALITÀ DI ACCESSO AL DOMINIO E AGLI APPLICATIVI

1. L'utente che ottiene l'accesso al dominio e agli applicativi è tenuto ad osservare il presente disciplinare e le altre norme disciplinanti le attività e i servizi che si svolgono via rete ed è tenuto a non commettere abusi e a non violare i diritti degli altri utenti e dei terzi.
2. L'utente che ottiene l'accesso al dominio e agli applicativi si assume la totale responsabilità delle attività svolte tramite la rete.
3. Qualsiasi accesso al dominio a agli applicativi viene associato ad una persona fisica cui imputare le attività svolte utilizzando il proprio account personale.
4. Al primo collegamento al dominio e agli applicativi, l'utente deve modificare la password comunicatagli dall'Amministratore di sistema e deve rispettare le seguenti regole:
Al primo accesso la password ottenuta dall'Amministratore di sistema deve essere cambiata.

- la password è segreta e non deve essere comunicata ad altri.
- la password va custodita con diligenza e riservatezza, in quanto stabilisce un rapporto biunivoco, che permette di responsabilizzare l'incarico stesso.
- la password deve essere costituita da una sequenza minima di otto caratteri alfanumerici e non deve essere facilmente individuabile, in particolare:
    - Non deve contenere nomi comuni
    - Non deve contenere nomi di persona
    - Deve comprendere almeno 3 fra questi 4 set di caratteri:
        - Lettere Maiuscole
        - Lettere Minuscole
        - Numeri
        - Simboli (quelli ammessi dal S.O.)
    - Deve essere diversa dallo User-Id
- La durata della parola chiave può variare da tre a sei mesi a seconda della criticità del sistema.

- L'utente deve comunicare all'Amministratore di sistema eventuale perdita della password in modo da bloccare l'account e provvedere alla reimpostazione della password.

TITOLO II

MISURE PER IL CORRETTO UTILIZZO DELLA POSTA ELETTRONICA E DELLA RETE INTERNET

ART. 9 - INTERNET: LA NAVIGAZIONE WEB

1. Il Comune di Refrontolo, datore di lavoro, può individuare categorie di siti considerati correlati o meno con la prestazione lavorativa. I siti considerati incoerenti saranno inseriti in una black list, e quindi non consultabili, su richiesta da parte del Direttore Generale.
2. Il sistema è già dotato di filtri per categoria. Se un URL rientra per errore in una categoria vietata, viene segnalato a video. Il dipendente è invitato a comunicarlo via e-mail all'Amministratore di sistema che lo inserirà nella "white list".
3. Il Comune di Refrontolo può configurare sistemi o utilizzare filtri che prevengano determinate operazioni – reputate incoerenti con l'attività lavorativa – quali l'upload e/o il download di file o software aventi particolari caratteristiche (dimensionali o di tipologia di dato).
5. Non è consentito il download di software o di file multimediali che non sia preventivamente autorizzato dai Responsabili di servizio, in accordo con l'Amministratore di sistema.
6. Il sistema provvede ad una adeguata registrazione nei log relativi alla navigazione internet dalle dotazioni informatiche collegate alla rete comunale.

ART. 10 - POSTA ELETTRONICA

1. L'indirizzo di posta elettronica è strumento di lavoro ed un bene messo a disposizione dell'utente per soli fini lavorativi. Le persone assegnatarie di indirizzo di posta elettronica sono responsabili del corretto utilizzo degli stessi.
2. E' buona norma evitare l'invio e la ricezione di messaggi personali dalla casella di posta elettronica assegnata dal Comune. A ciascun lavoratore, abilitato all'utilizzo della posta elettronica o all'accesso ad internet, saranno consentiti utilizzi a fini personali, esclusivamente dalla propria postazione, fuori dall'orario di lavoro o durante le pause, ed in ogni caso facendone un uso assolutamente limitato.
4. Le e-mail di provenienza non nota o palesemente provenienti da "spamming" devono essere immediatamente cancellate senza aprirle.
5. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili non destinati alla conservazione e allegati ingombranti.
6. Gli allegati inviati via posta elettronica non possono superare i 15 MB. Per inviare file di grandi dimensioni è necessario contattare l'Amministratore di sistema.
7. E' buona norma limitare lo scambio di dati sensibili, giudiziari, sanitari attraverso la posta elettronica. Qualora ciò si rendesse necessario, dovranno essere osservate le seguenti cautele:
   - verificare l'indirizzo di posta elettronica del destinatario;
   - non inserire dati sensibili nel corpo del messaggio;
   - inviare i dati sensibili come allegato del messaggio di posta elettronica che dovrà essere protetto con modalità idonee ad impedire l'illecita o fortuita acquisizione delle informazioni trasmesse da parte di soggetti diversi da quello cui sono destinati, che potranno consistere in una password per l'apertura del file o in una chiave crittografica rese note ai destinatari tramite canali di comunicazione differenti da quelli utilizzati per la spedizione dell'allegato.

8. Nello scambio di comunicazioni istituzionali va data priorità, ove possibile, all'utilizzo della posta elettronica certificata.

ART. 11 - CONTROLLI

1. Nell'effettuare controlli sull'uso degli strumenti elettronici, con particolare riferimento alle attività di cui al precedente art. 6, il Comune di Refrontolo evita un'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.
2. L'eventuale controllo è lecito solo se sono rispettati i principi di pertinenza e non eccedenza.
3. Nel caso in cui un evento dannoso o una situazione di pericolo non sia stato impedito con preventivi accorgimenti tecnici, il datore di lavoro può adottare eventuali misure che consentano la verifica di comportamenti anomali. Sarà preferito un controllo preliminare su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree.
4. Il controllo anonimo si concluderà 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 potrà essere circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia. In assenza di successive anomalie non è di regola giustificato effettuare controlli su base individuale.
5. L'accesso ai dati dei log, può essere fatto in forma graduale, in modo da considerarli in prima analisi in forma complessiva ed anonima, cioè non direttamente riconducibili ad un utente, salvo per gli utenti che si collegano direttamente ad internet bypassando il proxy server. Tali persone sono o gli addetti del sistema informatico quando devono diagnosticare problemi di rete o per motivi tecnici o gli utilizzatori delle dotazioni informatiche espressamente autorizzati per particolari motivi tecnici.
6. Non sono consentiti controlli prolungati, costanti o indiscriminati.

ART. 12 - APPARECCHIATURE PREORDINATE AL CONTROLLO A DISTANZA

1. Il datore di lavoro può riservarsi di controllare (direttamente o attraverso la propria struttura o incaricati esterni all'uopo autorizzati) l'effettivo adempimento della prestazione lavorativa e, se necessario, il corretto utilizzo degli strumenti di lavoro (cfr. artt. 2086, 2087 e 2104 cod. civ.).
2. Nell'esercizio di tale prerogativa occorre rispettare la libertà e la dignità dei lavoratori, in particolare per ciò che attiene al divieto di installare "apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori" (art. 4, primo comma, l. n. 300/1970), tra cui sono certamente comprese strumentazioni hardware e software mirate al controllo dell'utente di un sistema di comunicazione elettronica.
3. E' vietato il trattamento di dati personali mediante sistemi hardware e software che mirano al controllo a distanza di lavoratori svolti in particolare mediante:
a) 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;
b) la riproduzione e l'eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
c) la lettura e la registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
d) l'analisi occulta di computer portatili affidati in uso;
4. Il controllo a distanza vietato dalla legge riguarda l'attività lavorativa in senso stretto e altre condotte personali poste in essere nel luogo di lavoro. A parte eventuali responsabilità civili e penali, i dati trattati illecitamente non sono utilizzabili (art. 11, comma 2, del Codice).

ART. 13 - PROGRAMMI CHE CONSENTONO CONTROLLI "INDIRETTI"

1. Il datore di lavoro, utilizzando sistemi informativi per esigenze produttive o organizzative (ad es., per rilevare anomalie o per manutenzioni) o, comunque, quando gli stessi si rivelano necessari per la sicurezza sul lavoro, può avvalersi legittimamente, nel rispetto dello Statuto dei lavoratori ,art. 4, comma 2, di sistemi che consentono indirettamente un controllo a distanza (c.d. controllo preterintenzionale) e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori.

ART. 14 - CONSERVAZIONE

1. I sistemi software sono programmati e configurati in modo da cancellare periodicamente ed automaticamente i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.
2. In assenza di particolari esigenze tecniche o di sicurezza, la conservazione temporanea dei dati relativi all'uso degli strumenti elettronici deve essere giustificata da una finalità specifica e comprovata e limitata al tempo necessario e comunque nel rispetto delle indicazioni del Garante per la privacy.
3. L'eventuale ed eccezionale prolungamento dei tempi di conservazione potrà 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 o norma di legge.

In questi casi, il trattamento dei dati personali, tenendo conto, con riguardo ai dati sensibili, delle prescrizioni contenute nelle autorizzazioni generali adottate dal Garante, dovrà essere limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed essere effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità già esplicitati.

ART. 15 - SISTEMI ELETTRONICI DI REGISTRAZIONE DELLE ATTIVITÀ NEL SISTEMA INFORMATICO.

1. Nel sistema informatico del Comune di Refrontolo, sono presenti i seguenti servizi che possono dare informazioni sulle attività svolte dagli utenti nella rete, sia essa intranet o internet ;

- Proxy e Firewall.
  - Filtro e registrazione di accesso ad internet e sistema per il blocco dei tentativi di intrusione dall'esterno. (E' presente un archivio dove viene registrato tutto il traffico tra la rete intranet ed internet)
- Log del server di Dominio.
  - Archiviazione degli accessi al sistema informatico e registrazione attività sulla rete intranet.
- Log nel server di Posta Elettronica.

ART. 16 - PERMESSI DI ACCESSO AI LOG

1. Le informazioni di cui sopra possono essere visionate dalle autorità competenti in caso di indagini.
2. Le stesse informazioni sono potenzialmente visibili all'amministratore di sistema, il quale, per garantire sia la privacy degli utilizzatori, sia il corretto funzionamento del sistema ed un certo livello di sicurezza, può visionare:

- Log del Proxy e Firewall.
- Log del server di Dominio.

- Log del server di Posta, limitatamente al controllo del corretto funzionamento dello stesso.

e non può visionare:

- Posta elettronica salvata nel server di Posta.
- Log del server di Posta, per quanto concerne il singolo evento di ricezione/spedizione di posta (se non espressamente richiesto dall'interessato stesso)

ART. 17 - SANZIONI

1. 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.

ART. 18 - NORMA FINALE

1. Il presente disciplinare abroga ogni provvedimento precedente che disciplina la materia.