COMUNE DI PERDAXIUS
PROVINCIA DI CARBONIA-IGLESIAS

Allegato alla Deliberazione della G.C. n. 59 del 28.07.2008

Disciplinare interno sulle norme di comportamento per l'accesso e l'utilizzo dei sistemi informativi, delle risorse informatiche, del servizio Internet e del servizio di posta elettronica del Comune di PERDAXIUS

Il presente Disciplinare, adottato con Deliberazione della Giunta Comunale, tiene conto delle indicazioni e delle prescrizioni contenute nella Deliberazione del Garante per la protezione dei dati personali del 1 Marzo 2007 n. 13, recante "Linee guida del Garante per posta elettronica ed internet" e ha per oggetto i criteri e le modalità operative per l'accesso e l'utilizzo dei sistemi informativi, delle risorse informatiche, del servizio Internet e di posta elettronica da parte dei dipendenti dell'Ente e di tutti gli altri soggetti che a vario titolo prestano servizio o attività per conto e nelle strutture del Comune di PERDAXIUS (LSU, tirocinanti, collaboratori).

DEFINIZIONI

- **TITOLARE DEL TRATTAMENTO DEI DATI**: secondo quanto espressamente previsto dall'art. 28 D. Lgs. 196/03 "quando il trattamento è effettuato da una persona giuridica, da una Pubblica Amministrazione o da qualsiasi altro ente, Titolare del trattamento è l'entità nel suo complesso (…)".

Il Provvedimento a carattere generale del Garante per la Protezione dei Dati Personali, del 14/06/07 (G.U. n. 161 del 13/07/07), recante "Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico", precisa definitivamente che in ambito pubblico "per individuare il Titolare del trattamento, occorre far riferimento all'amministrazione o ente centrale o locale nel suo complesso, anziché a singole articolazioni interne o alle persone fisiche che l'Amministrano o la rappresentano (ad esempio, il ministro, il direttore generale o il presidente).

Il Titolare del trattamento dei dati è dunque l'Ente nel suo complesso e non i singoli soggetti fisici che operano al suo interno. Sarà dunque l'Ente, che dovrà adempiere alle disposizioni contenute nel Codice della Privacy (D. Lgs. 196/03).

- **RESPONSABILE DEL TRATTAMENTO DEI DATI**: il Titolare del trattamento dei dati, la Giunta Comunale con proprio atto deliberativo, individua all'interno dell'Ente i Responsabili del trattamento dei dati che coincidono con i Responsabili di Area in cui si articola l'Ente e attribuisce formalmente mandato al Sindaco pro tempore di formalizzare con apposito decreto la loro designazione.
- **INCARICATI DEL TRATTAMENTO DEI DATI**: sono tutti i soggetti che operano all'interno dell'Ente ponendo in essere delle operazioni di trattamento di dati, espressamente designati con atto scritto (Determinazione del Responsabile del trattamento dei dati) che individua puntualmente l'ambito del trattamento consentito.
- **UTENTE INTERNET**: persona, all'interno dell'Ente, autorizzata ad accedere al servizio internet per la navigazione;
- **UTENTE DI POSTA ELETTRONICA**: persona, all'interno dell'Ente, autorizzata ad accedere al servizio di posta elettronica;
- **WHITE LIST**: elenco di siti direttamente e immediatamente accessibili da parte di tutti gli utenti internet;
- **BLACK LIST**: elenco di siti non accessibili da nessun utente;
- **INTERNET PROVIDER:** azienda che fornisce al Comune il canale di accesso alla rete internet;
- **POSTAZIONE DI LAVORO**: personal computer collegato alla rete comunale tramite il quale l'utente accede ai servizi;
- **LOG:** archivio delle attività di consultazione in rete.

CAPO 1
UTILIZZO DEL PERSONAL COMPUTER

1.1 Il Personal Computer (PC) affidato al dipendente è uno strumento di lavoro. Ogni utilizzo non inerente l'attività lavorativa può contribuire ad innescare disservizi, costi ulteriori di manutenzione e minacce alla sicurezza dei dati trattati dall'Ente.
I dipendenti devono custodire la propria strumentazione in modo diligente, segnalando con tempestività ogni danneggiamento, avaria, furto o smarrimento al proprio Responsabile di Area.

1.2 L'accesso a ciascun PC è protetto da credenziale di autenticazione costituita da una User ID (codice per l'identificazione dell'incaricato) associata a una PASSWORD riservata (parola chiave), conosciuta esclusivamente dal medesimo incaricato.

1.3 Gli Incaricati del trattamento dei dati sono responsabili della custodia e dell'utilizzo diligente e consapevole delle proprie credenziali di autenticazione che devono essere gestite attenendosi alle seguenti istruzioni:

a) La parola chiave, assegnata a ciascun incaricato, è composta da un numero minimo di otto caratteri alfanumerici.

b) La parola chiave assegnata, deve essere prontamente e autonomamente sostituita dall'incaricato al primo utilizzo e successivamente modificata con cadenza almeno semestrale ovvero trimestrale nell'ipotesi di trattamento di dati sensibili o giudiziari.

c) All'interno di ciascuna Area in cui si articola l'Ente, la parola chiave deve essere consegnata, in busta chiusa, al Responsabile del trattamento dei dati affinché proceda alla custodia delle credenziali.

d) La password non deve contenere riferimenti, diretti o indiretti, agevolmente riconducibili all'incaricato.

e) L'incaricato, nella scelta della propria password, deve utilizzare anche caratteri speciali e lettere maiuscole e minuscole.

f) La parola chiave deve essere custodita con la massima attenzione e segretezza e non deve essere divulgata o comunicata a terzi.

g) L'incaricato è responsabile di ogni utilizzo indebito o non consentito della parola chiave di cui sia titolare.

h) Qualora, in caso di prolungata assenza o impedimento dell'incaricato, così come espressamente prevede la Regola 10 contenuta nell'Allegato B al D. Lgs. 196/03, ci sia la necessità di accedere ai dati e agli strumenti elettronici per esigenze di operatività e di sicurezza del sistema, è necessario presentare una richiesta scritta e motivata al Responsabile del trattamento dei dati (che coincide con il Responsabile dell'Area) il quale, al rientro in servizio dell'incaricato assente ovvero impedito, provvederà ad informarlo dell'accaduto affinché si possa procedere, senza indugio, alla sostituzione della parola chiave.

i) Le credenziali di autenticazione individuali per l'accesso all'elaboratore ovvero alle applicazioni, non devono mai essere condivise tra più utenti (anche se Incaricati del trattamento). Se un utente dovesse avere la necessità di trattare gli stessi dati o di usare le stesse procedure alle quali può accedere un collega, dovrà richiedere, al Responsabile del Servizio Informatico ovvero al personale all'uopo preposto, che gli siano assegnate le proprie credenziali di autenticazione, dotate dei privilegi necessari all'accesso ai dati o ai servizi richiesti.

l) Se l'incaricato sospetta che le proprie credenziali di autenticazione abbiano perso il requisito della segretezza (ad es. perché crede che queste siano conosciute anche da altri colleghi) è tenuto immediatamente a procedere al cambio della parola chiave.

1.4 Il dipendente, preso atto che, la conoscenza della password da parte di terzi consente agli stessi l'accesso all'elaboratore, l'utilizzo dei relativi servizi in nome dell'utente titolare e l'accesso ai dati cui il medesimo è abilitato, con possibilità di gestione degli stessi (visualizzazione di informazioni riservate, distruzione o modifica dei dati, lettura della propria posta elettronica, uso indebito di servizi ecc.), si impegna a:

- non consentire, una volta superata la fase di autenticazione, l'uso della propria postazione di lavoro a personale non autorizzato, in particolar modo per quanto riguarda l'accesso a internet e ai servizi di posta elettronica;

- non lasciare incustodita ed accessibile la propria postazione una volta che sia avvenuta l'autenticazione con le proprie credenziali;
- conservare e custodire la password nella massima riservatezza e con la massima diligenza;
- non utilizzare credenziali (user-id e password) di altri utenti, nemmeno se fornite volontariamente o di cui si sia venuti casualmente conoscenza;
- mantenere la corretta configurazione del proprio elaboratore non alterando le componenti hardware e software predisposte allo scopo né installando ulteriori software non autorizzati.

1.5 Qualunque azione o attività posta in essere mediante l'utilizzo del codice identificativo e della password assegnate, è attribuita in via esclusiva all'utente assegnatario delle credenziali di autenticazione che sarà chiamato a rispondere delle attività eseguite.
L'utente è civilmente responsabile di qualsiasi danno arrecato al Comune, all'internet provider e/o a terzi in violazione di quanto espressamente previsto dalla norma e di quanto indicato nel presente disciplinare.
L'utente può essere chiamato a rispondere, oltre che per i propri fatti illeciti, anche per quelli commessi da chiunque utilizzi il suo codice identificativo e la sua parola chiave, con particolare riferimento all'immissione in rete di contenuti critici o idonei a offendere l'ordine pubblico e il buon costume così come definiti dalla giurisprudenza più recente.
La violazione delle presenti disposizioni può comportare infine l'applicazione delle sanzioni disciplinari previste dal vigente Contratto Collettivo di Lavoro, rimanendo ferma ogni ulteriore forma di responsabilità penale.
1.6 Non è consentito installare autonomamente programmi provenienti dall'esterno senza la preventiva autorizzazione del Responsabile del Servizio informatico dell'Ente.
In caso di necessità di acquisto o di dotazione di programmi applicativi e procedure pertinenti esclusivamente una o più Aree, sarà necessario preventivamente richiedere e acquisire l'autorizzazione in forma scritta da parte del Responsabile del Servizio informatico dell'Ente, per garantire la compatibilità funzionale, tecnica ed il mantenimento dell'efficienza operativa dei sistemi e della Rete.
1.7 Non è consentito ai dipendenti modificare le caratteristiche impostate sui PC assegnati, le configurazioni della rete LAN presente nella sede dell'Ente e la configurazione del Browser per la navigazione, salvo esplicita autorizzazione del Responsabile del Servizio informatico, ovvero altro personale all'uopo preposto.
1.8 Ciascun Responsabile del trattamento dei dati vigila sul corretto e coerente utilizzo delle risorse informatiche assegnate all'interno di ciascuna Area/Servizio al fine di evitare che le stesse vengano utilizzate impropriamente ovvero possano formare oggetto di accesso da parte di personale non espressamente autorizzato.
1.9 Il Personal Computer deve essere spento al termine della propria attività lavorativa, prima di lasciare l'ufficio oppure in caso di assenza prolungata dall'ufficio stesso.
Lasciare infatti un elaboratore incustodito potrebbe essere causa di utilizzo improprio da parte di terzi senza che per l'Ente ci sia la possibilità di fornire la prova dell'indebito uso.
1.10 Non è consentita l'installazione sul proprio PC di nessun dispositivo di memorizzazione, comunicazione o altro (masterizzatore, modem) se non con l'espressa autorizzazione del Responsabile del Servizio informatico, ovvero altro personale all'uopo preposto, previa richiesta scritta da parte del Responsabile del trattamento dei dati dell'Area cui è assegnato l'elaboratore.
1.11 Ai dipendenti individuati quali Incaricati del trattamento dei dati è fatto obbligo di provvedere a distruggere i supporti rimovibili su cui sono memorizzati dati sensibili o giudiziari (nastri, floppy disk, CD Rom) non più utilizzati.
1.12 Ogni dipendente deve prestare la massima attenzione ai supporti di memorizzazione di origine esterna, avvertendo senza indugio il Responsabile del Servizio informatico dell'Ente ovvero altro personale all'uopo preposto, nel caso in cui si dovesse rilevare la presenza di virus ed attenendosi scrupolosamente alla procedura disciplinata dal paragrafo 3.1 del presente disciplinare interno, relativo alle procedure di protezione Antivirus.
1.13 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 o politica.
1.14 E' parimenti vietato utilizzare gli strumenti informatici comunali al fine di custodire, far

circolare ovvero promuovere, materiale pubblicitario personale, codice maligno (virus, trojan horses, programmi non licenziati) e ogni altra tipologia di materiale non autorizzato.
1.15 E' vietato copiare, scaricare ovvero mettere a disposizione di altri materiale protetto dalla legge sul diritto di autore (documenti, files musicali, film e filmati) di cui l'Ente non abbia acquisito i diritti.
1.16 E' vietato rimuovere, danneggiare deliberatamente ovvero asportare componenti hardware.

CAPO 2
UTILIZZO DI PC PORTATILI

2.1 Il dipendente al quale sia stato assegnato dall'Amministrazione un elaboratore portatile, è responsabile dello stesso e deve custodirlo con diligenza sia durante gli spostamenti che durante l'utilizzo nel luogo di lavoro.
2.2 Ai PC portatili si applicano le stesse regole di utilizzo previste per i PC fissi connessi in Rete.

CAPO 3
BACK-UP

3.1 Salvo che non sia previsto un sistema di salvataggio di dati personali automatico ovvero centralizzato, ciascun dipendente deve procedere, con riferimento a tutti i documenti e le Banche Dati non coperti dalla indicata procedura di sicurezza, alla effettuazione di copie di back-up dei dati personali oggetto di trattamento, con cadenza almeno settimanale, utilizzando gli apparati ed i supporti che siano messi a disposizione dell'Incaricato, avendo cura di custodire i citati supporti di memorizzazione utilizzati, all'interno di un contenitore (armadio, cassetto, cassettiera) munito di serratura, in locale idoneo (protetto da fonti di calore, campi magnetici, interferenze elettromagnetiche , intrusioni, incendi ed allagamenti), separato da quello in cui è ubicata l'unità di elaborazione utilizzata per il trattamento, al quale possano accedere esclusivamente i Responsabili, gli Incaricati o l'Amministratore del Sistema Informatico dell'Ente, se individuato.

CAPO 4
INTERNET

4.1 Il PC abilitato alla navigazione in Internet costituisce uno strumento necessario allo svolgimento dell' attività lavorativa. E' proibita la navigazione in Internet per motivi diversi da quelli funzionali all'attività lavorativa stessa.
4.2 Tutti i dipendenti cui è assegnata dal Comune una postazione di lavoro possono utilizzare Internet. Prossimamente, l'Ente provvederà a circoscrivere la navigazione limitatamente ad una lista di siti preventivamente individuati dal Comune (WHITE LIST) e previa identificazione dell'utente con le modalità precedentemente illustrate (credenziali di autenticazione costituite da ID UTENTE e PASSWORD).
4.3 La lista dei siti fruibili (WHITE LIST) verrà progressivamente implementata e completata nel tempo ed il novero di tali siti, sarà deciso di concerto dai Responsabili di Area dell'Ente unitamente al Responsabile del Sistema informatico e del Segretario Comunale.
4.4 L'utilizzo ampio di Internet, non limitato cioè alla lista di siti individuata come sopra (WHITE LIST), è autorizzata per ogni singolo utente da ciascun Responsabile del trattamento dei dati.
I responsabili delle Aree in cui si articola l'Ente sono autorizzati automaticamente a tale tipo di accesso non limitato.
4.5 In ogni caso, al fine di prevenire il rischio di utilizzi impropri della rete reputati non compatibili con l'attività lavorativa, il Comune utilizza un sistema di filtri che impediscono l'accesso diretto a siti che non hanno alcuna utilità per l'attività lavorativa (BLACK LIST).
Oltre a tale sistema, è costantemente attiva una funzione di verifica del contenuto del sito; ove tale contenuto, secondo l'impostazione di una soglia predefinita, appaia non funzionale all'attività lavorativa, viene visualizzato un messaggio che avverte l'utente; l'utente può quindi

annullare la richiesta di accesso ovvero accedere al sito, previa dichiarazione di responsabilità, rendendolo da quel momento disponibile a tutti gli utenti Internet.
Le modalità di individuazione e di applicazione dei filtri sono decise di concerto dai Responsabili di Area dell'Ente unitamente al Responsabile del Sistema informatico ed al Segretario Comunale.
4.6 Ciascun dipendente è direttamente e personalmente responsabile dell'uso del servizio di accesso a Internet, dei contenuti che vi ricerca, dei siti che contatta, delle informazioni che vi immette e delle modalità con cui opera.
4.7 E' 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 espressamente autorizzati o attinenti i compiti e le mansioni assegnate e con il rispetto delle normali procedure di acquisto.
4.8 E' vietata ogni forma di registrazione a siti o a mailing list i cui contenuti non siano legati allo svolgimento dell'attività lavorativa istituzionale.
4.9 E' vietata la partecipazione a Forum, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (ovvero nicknames) se non strettamente attinenti l'attività lavorativa svolta.
4.10 E' vietata tassativamente la navigazione in siti da cui sia possibile evincere le opinioni politiche, religiose, filosofiche e sindacali o le abitudini sessuali dell'utilizzatore; non è consentito inoltre visitare siti e memorizzare documenti informatici dai contenuti oltraggiosi, discriminatori ovvero che offendono il comune senso del pudore.
4.11 Al dipendente non è consentito:
- servirsi o dar modo ad altri di servirsi della stazione di accesso a internet per attività non istituzionali, per attività poste in essere in violazione del diritto d'autore o altri diritti tutelati dalla normativa vigente;
- scaricare software dalla rete se non espressamente autorizzato dal Responsabile del Servizio Informatico dell'Ente;
- utilizzare internet provider diversi da quello ufficiale del Comune e connettere stazioni di lavoro aziendali alle reti di tali provider con sistemi di connessione diversi (es. modem) da quello centralizzato;
- usare la rete in modo difforme da quanto previsto dal presente documento e dalle leggi penali, civili e amministrative in materia di disciplina dell'attività e dei servizi svolti sulla rete.

CAPO 5
POSTA ELETTRONICA

5.1 L'utilizzo del servizio di posta elettronica è consentito solo per ragioni di servizio agli utenti identificati con le modalità precedentemente illustrate, ai quali il Comune assegna una casella di posta personale e nominativa.
5.2 La casella di posta elettronica istituzionale è uno strumento di lavoro che deve pertanto essere utilizzato esclusivamente per esigenze connesse all'attività lavorativa. Non sono ammessi utilizzi diversi o privati dell'indirizzo. I dipendenti ai quali è assegnata, sono responsabili del corretto utilizzo della stessa.
5.3 Si evidenzia che, esclusi i casi in cui sia possibile avvalersi di una utenza di posta elettronica certificata unitamente alla apposizione della firma digitale sul documento trasmesso, i sistemi di posta elettronica non consentono di garantire circa la riservatezza delle informazioni trasmesse. Per questa ragione, si raccomanda ai dipendenti di non inoltrare, con questo mezzo, informazioni e dati classificabili come "sensibili" ovvero "giudiziari" ai sensi dell'art.4, comma 1, lettere d,e D. Lgs. 196/03.
5.4 E' fatto divieto di utilizzare le caselle di posta elettronica istituzionale per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list non attinenti la propria attività svolta per l'Ente, salvo diversa esplicita autorizzazione in tal senso.
5.5 La casella di posta elettronica deve essere mantenuta in ordine, cancellando periodicamente i documenti inutili e gli allegati ingombranti.
5.6 E' vietato utilizzare il servizio di posta elettronica istituzionale per inoltrare catene telematiche, appelli, petizioni, giochi, scherzi, barzellette, e altre e-mails che non abbiano

attinenza con l' attività lavorativa. Se si dovessero ricevere messaggi di tale tipo, è necessario informare con immediatezza il Responsabile del Sistema Informatico. In ogni caso, è fatto espresso divieto di attivare gli allegati di tali messaggi.
5.7 E' vietato utilizzare tecniche di "mail spamming" cioè di invio massiccio di comunicazioni a liste di utenti non istituzionali. E' parimenti vietato, allegare al testo delle comunicazioni materiale potenzialmente insicuro (programmi, macro, scripts).
5.8 Al fine di recepire le linee guida dettate dal Garante per la protezione dei dati personali in materia di posta elettronica nel rapporto di lavoro, l'Ente provvederà a mettere a disposizione di ciascun dipendente apposite funzionalità di sistema, di agevole utilizzo, che consentano di inviare automaticamente, in caso di assenza programmata dal servizio dell'utente, messaggi di risposta che avvisino il mittente dell'assenza del destinatario, individuando eventualmente altre modalità di contatto con la struttura (coordinate elettroniche o telefoniche di un altro soggetto o altre utili modalità di contatto con la struttura).
In caso di assenza non programmata e nelle more dell'attivazione della procedura di cui sopra, l'utente può delegare un altro dipendente dell'ufficio (fiduciario) a verificare il contenuto dei messaggi e ad inoltrare al Responsabile dell'Area quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa dell'Ufficio.

CAPO 6
MONITORAGGIO E CONTROLLI

6.1 Il Comune può avvalersi di sistemi di controllo sul corretto utilizzo degli strumenti di lavoro (che consentono indirettamente un controllo a distanza dell'effettivo adempimento della prestazione lavorativa e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori) esclusivamente nel rispetto di quanto previsto dal Provvedimento del Garante per la protezione dei dati personali del 1 marzo 2007 n. 13, di quanto disposto dagli artt. 2 e 15 della Costituzione, dall'art. 616, quarto comma, c.p. e dall'art. 49 del Codice dell'amministrazione digitale.

6.2 In particolare l'Ente, nell'effettuare controlli sull'uso degli strumenti elettronici eviterà 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.

6.3 Le comunicazioni effettuate attraverso il servizio di posta elettronica sono riservate. Il contenuto di tali comunicazioni non può in nessun caso essere oggetto di alcuna forma di verifica, controllo o censura da parte del Comune, dell'internet provider o da parte di altri soggetti.

6.4 Le dichiarazioni di responsabilità effettuate dagli utenti Internet per visualizzare e rendere da quel momento disponibile il sito/dominio, secondo quanto disposto dal punto 4.5 del presente Disciplinare, sono a disposizione del Responsabile del Sistema Informatico dell'Ente.

6.5 Le attività sull'uso del servizio di accesso ad Internet vengano automaticamente registrate in forma elettronica attraverso i LOG di sistema. Il trattamento dei dati contenuti nei LOG, può avvenire esclusivamente in **forma anonima** in modo tale da precludere l'identificazione degli utenti e/o delle loro attività.

6.6 I dati anonimi aggregati, riferibili all'intera struttura o a sue Aree, sono a disposizione dell'Ufficio Personale e del Responsabile del Sistema Informatico per le valutazioni di competenza che riguardano:

- per ciascun sito/dominio visitato le informazioni sul numero di utenti che lo visitano, sul numero delle pagine richieste e sulla quantità dei dati scaricati;
- per ciascun utente le informazioni sul numero di siti visitati, sulla quantità totale di dati scaricati e sulle postazioni di lavoro utilizzate per la navigazione.

6.7 I **dati personali** contenuti nei LOG possono essere trattati esclusivamente in via eccezionale e nelle ipotesi tassativamente di seguito indicate:
- per rispondere ad eventuali richieste della polizia postale e/o dell'autorità giudiziaria;

- su richiesta del Responsabile del Servizio Informatico, ovvero di personale all'uopo preposto, limitatamente al caso di utilizzo anomalo degli strumenti informatici da parte degli utenti di una specifica Area o servizio (rilevabile esclusivamente dai dati aggregati) reiterato nel tempo, nonostante un esplicito avviso circoscritto e rivolto ai dipendenti afferenti all'Area o servizio coinvolto e un espresso invito agli stessi utenti ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite.

6.8 I dati contenuti nei LOG sono conservati per il tempo strettamente necessario al perseguimento di finalità organizzative, produttive e di sicurezza, comunque non superiore a 90 giorni, e sono periodicamente cancellati automaticamente dal sistema.
6.9 I dati riguardanti il software installato sulle postazioni di lavoro (senza alcuna indicazione dell'utente che ha effettuato l'installazione) possono essere trattati per finalità di verifica della sicurezza dei sistemi ed il controllo del rispetto delle licenze regolarmente acquistate.

CAPO 7
INTERRUZIONE E CESSAZIONE D'UFFICIO DEL SERVIZIO DI ACCESSO AD INTERNET

Eventuali interruzioni del servizio di accesso ad Internet sono comunicate agli utenti.
Ai sensi del presente Disciplinare interno, l'utilizzo del servizio di accesso ad internet cessa d'ufficio nei seguenti casi:

- se non sussiste più la condizione di dipendente o di collaboratore autorizzato all'uso;
- se è accertato un uso non corretto del servizio da parte dell'utente o comunque un uso estraneo ai suoi compiti istituzionali;
- se vengono sospettate manomissioni e/o interventi sull'hardware e/o sul software dell'utente impiegati per la connessione compiuti eventualmente da personale non autorizzato;
- in caso di accesso dell'utente a directory, a siti e/o file e/o servizi da chiunque resi disponibili non rientranti fra quelli per lui autorizzati;
- in caso di concessione di accesso ad internet diretta o indiretta a qualsiasi titolo da parte dell'utente a terzi;
- in ogni altro caso in cui sussistono ragionevoli evidenze di una violazione degli obblighi dell'utente.