AZIENDA PUBBLICA DI SERVIZI ALLA PERSONA
Riva del Garda – Provincia autonoma di Trento

Riva del Garda 10 febbraio 2016

REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI

Approvato con Delibera n. 5 del 10 febbraio 2016 prot. 305 dell'11/02/2016

INDICE

REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI

PREMESSA

La A.P.S.P. "CASA MIA", con sede in viale Trento n. 26, 38066 Riva del Garda (TN) mette a disposizione dei propri ospiti e/o utenti e degli altri soggetti autorizzati una serie di strumenti informatici (PC, rete, connessione ad internet, ecc.) per consentire la soddisfazione di esigenze connesse alle attività di assistenza e educazione e avviamento professionale fornite.

La A.P.S.P. "CASA MIA intende di conseguenza definire le modalità d'uso dei predetti strumenti informatici nel giusto contemperamento fra i diritti dei soggetti coinvolti e l'osservanza delle disposizioni in materia di trattamento dati personali e sicurezza informatica.

Ai sensi del Codice in materia di protezione dei dati personali (D.Lgs. 196/2003) l'utilizzo di sistemi informatici o telematici deve infatti avvenire attraverso la massima cautela e in osservanza delle disposizioni tecniche di cui al predetto Codice.

L'utilizzo di tutti gli strumenti informatici di proprietà del presente Ente deve avvenire osservando scrupolosamente le regole di buona diligenza e prudenza, con senso di responsabilità e seguendo le istruzioni impartite dal Direttore, dagli Assistenti e dalle persone da essi delegate.
L'uso degli strumenti (*PC, attrezzatura informatica e aule didattiche, notebook, rete, ecc*.) è consentito unicamente agli utenti autorizzati dal Direttore ovvero dai Responsabili della gestione della struttura informatica.
L'accesso agli strumenti è consentito solo previa autenticazione personale effettuata mediante sistema di identificazione (attribuzione individuale di nome utente e password). Le politiche di gestione delle password dovranno rispettare il dettato normativo in materia di privacy e sicurezza informatica.
In ogni caso, ciascun utente è personalmente responsabile per l'uso del proprio *account* ed è tenuto a tutelarlo da accessi non autorizzati. Non è di conseguenza ammessa la comunicazione del proprio *account* a terzi.
Le disposizioni di seguito riportate, relative alle credenziali di autenticazione, contribuiranno a garantire la sicurezza nell'accesso.
Ogni utente è tenuto a scegliere una password composta da almeno 8 caratteri alfanumerici, che non contenga riferimenti che riconducano agevolmente all'incaricato (es: non inserire nome o cognome proprio e di familiari).
La password è personale, riservata e non può essere ceduta o comunicata ad alcuno. E' pertanto vietato l'uso della password di altri utenti; qualora se ne venisse a conoscenza è obbligatorio segnalare il fatto all'utente interessato, al docente responsabile e all'amministratore.
E' obbligatorio modificare la password ogni volta che il sistema ne faccia richiesta.

Per esigenze operative o di sicurezza e integrità del sistema e dei dati, l'amministratore di sistema ha facoltà di modificare la password degli utenti.
Qualsiasi attività svolta utilizzando l'account attribuito sarà ricondotta nella sfera di responsabilità dell'utente assegnatario del codice. Si segnala che ogni utente è civilmente responsabile per i danni cagionati all'Ente, all'Internet Provider e/o a terzi, non solo in relazione ai propri fatti illeciti ma anche per quelli commessi da chiunque utilizzi il suo codice utente e password.

L'uso dei PC ubicati nelle aule e nei laboratori e dei relativi programmi, compatibilmente con i fini didattici, deve preferibilmente avvenire in modo tale da non salvare in cartelle condivise dati personali e riservati, se non per fini strettamente necessari.
L'accesso alla rete internet mediante le strutture informatiche dell'Istituto deve essere finalizzato al perseguimento di fini connessi all'attività di educazione e assistenza e avviamento professionale degli ospiti e/o utenti.
Non è consentito accedere ed utilizzare la rete internet in modo difforme da quanto previsto dal presente disciplinare e, ovviamente, dalle leggi penali, civili ed amministrative in materia. In ogni caso, ogni utente è direttamente responsabile dell'uso del servizio di accesso ad Internet, dei siti ai quali accede, delle informazioni che immette e riceve.

Qualora un utente dovesse riscontrare malfunzionamenti, guasti o situazioni di rischio per la sicurezza o l'integrità del sistema causati da comportamento doloso o comunque non conforme alle istruzioni e disposizioni è tenuto a darne immediata comunicazione ad un docente responsabile.

E' severamente vietato:

Utilizzare le attrezzature informatiche messe a disposizione dall'Ente per scopi diversi da quelli afferenti fini connessi alla attività di educazione e assistenza e avviamento professionale.
Svolgere operazioni di loading (caricamento) e downloading (scaricamento) non autorizzate o non rientranti nei fini predetti.
Salvare in cartelle condivise file contenenti dati personali o informazioni riservate.
Modificare le configurazioni dei PC ubicati nella sede dell'Ente.

Il personale e i tecnici informatici sono tenuti a vigilare sul corretto utilizzo delle attrezzature informatiche ed hanno il dovere di informare senza ritardo la Direzione sull'eventuale utilizzo improprio dei sistemi, dei PC e dei relativi programmi.

Nel caso in cui si ravvisasse un utilizzo improprio delle predette attrezzature, la Direzione si riserva ogni idoneo provvedimento in linea con le politiche di gestione elaborate nel presente regolamento, tra cui:

- poter controllare gli accessi alle strutture, ivi compreso il corretto utilizzo di elaboratori, programmi e sistemi operativi, in linea con le presenti regole di utilizzo e nel rispetto delle disposizioni di cui al d.lgs. n. 196/2003;

- poter procedere alla rimozione di ogni file estraneo pericoloso per la sicurezza del sistema, non attinente all'attività didattica o acquisito ed installato in violazione di principi generali di buona condotta o delle norme in materia di copyright e diritto d'autore.

- adottare un sistema generale di controllo e prevenzione sugli accessi alla rete e di limitazione all'uso della stessa, anche tramite il divieto di navigazione su determinati siti (mediante accessi limitati e filtri per categorie di utenti);

- implementare costantemente le misure di sicurezza indicate dal Disciplinare Tecnico in materia di Misure Minime di Sicurezza di cui all'allegato B) del D.lgs. n. 196/2003, ivi compreso il Documento Programmatico sulla Sicurezza che viene aggiornato periodicamente ed è messo a disposizione per la consultazione degli utenti che ne facciano richiesta;
- sospendere, anche selettivamente, il servizio di accesso ad Internet nei seguenti casi:

- esigenze di manutenzione;
- accertamento di un uso non corretto del servizio da parte dell'utente;
- in caso di manomissioni e/o interventi su hardware/software;
- diffusione o comunicazione imputabili direttamente o indirettamente all'utente relativamente a profili d'accesso o altre informazioni riservate;
- accesso a directory/file/siti non rientranti fra quelli per cui l'utente abbia autorizzazione.

Sul web gli ospiti non devono di norma rivelare i propri dati personali (nome, cognome, indirizzo, numero di telefono personale, ecc.).

Gli utilizzatori delle postazioni non possono relazionarsi autonomamente con altri soggetti (chat, social network, ecc.) senza il permesso degli personale di riferimento. Ogni comportamento difforme rientrerà nella sfera della diretta responsabilità dell'utente.

Senza diversa autorizzazione è permesso solo l'accesso ai collegamenti consentiti mediante l'impostazione del sistema di autenticazione.

Agli utilizzatori di norma non è permesso accedere a *newsgroup* e *chat room*.

L'accesso ad Internet può essere filtrato attraverso un *proxy server* che scherma alla fonte i siti inidonei – questo servizio può essere disabilitato solo dall'amministratore di sistema.

Ciò premesso, l'Ente può avvalersi di sistemi controllo relativi al corretto utilizzo degli strumenti indicati: tali controlli saranno effettuati qualora le misure minime preventivamente esposte non siano state sufficienti per evitare comportamenti anomali. I controlli saranno svolti con gradualità, secondo i principi di pertinenza e non eccedenza. In seguito si espongono le modalità di tali controlli:

- in prima battuta si effettuerà un controllo preliminare su dati anonimi ed aggregati; si procederà pertanto con verifiche di rete o gruppo;
- il controllo anonimo può terminare con un avviso di rilevazione di un utilizzo inadeguato degli strumenti indicati; contestualmente si diramerà una nota di richiamo invitando gli utenti ad attenersi alle regole elaborate;
- se si dovesse ripetere l'anomalia, sarà facoltà dell'Ente procedere con controlli più mirati, anche su base individuale ed assumere ogni idoneo e conseguente provvedimento.

I dati contenuti nei file di log, relativi agli accessi ad Internet e al traffico telematico, possono essere conservati per il tempo strettamente necessario al perseguimento di finalità organizzative e di sicurezza. I file di log potranno essere utilizzati in tali casi:
- produzione di report statistici che presentino i dati relativi alla navigazione in forma aggregata e anonima;
- analisi dei problemi riscontrati nel sistema e soluzione dei medesimi, estraendo i dati in modo aggregato e in forma anonima

Per ogni chiarimento sarà possibile rivolgersi all'amministratore di sistema (Pernici Paolo o al Direttore (Galvagni Renzo)

LINEE GUIDA PER L'UTILIZZO DI INTERNET E POSTA ELETTRONICADA PARTE DEI DIPENDENTI.

1. OGGETTO

Il presente disciplinare, adottato sulla base delle indicazioni contenute nel provvedimento generale del Garante per la protezione dei dati personali di data 1 marzo 2007, n. 13 ("Lavoro: le linee guida del Garante per posta elettronica e internet", G.U. n. 58 del 10 marzo 2007) ha per oggetto i criteri e le modalità operative di accesso ed utilizzo del servizio Internet e posta elettronica da parte dei dipendenti della A.P.S.P. "CASA MIA", con sede in viale Trento n. 26, 38066 Riva del Garda (TN), e di tutti gli altri soggetti che a vario titolo operano nella struttura. (lavoratori socialmente utili, collaboratori, tirocinanti, etc…).
La A.P.S.P. "CASA MIA", quale titolare del trattamento dati, deve definire le modalità d'uso degli strumenti informatici dell'Ente (Internet e posta elettronica), tenendo conto dei diritti dei lavoratori e della disciplina in tema di relazioni sindacali: si devono a tal proposito bilanciare gli interessi relativi alla prevenzione di usi arbitrari degli strumenti informatici, con la riservatezza dei lavoratori.

2. DEFINIZIONI

Nel presente documento si intende per:

- POSTAZIONE DI LAVORO: personal computer, PC portatile, WBT o thin client collegato alla rete informatica dell'Ente tramite il quale l'utente accede ai servizi informatici.
- UTENTE DI POSTA ELETTRONICA: persona autorizzata ad accedere al servizio di posta elettronica.
- LOG: archivio delle attività effettuate in rete dall'utente.
- INTERNET PROVIDER: azienda che fornisce il canale d'accesso alla rete Internet.
- CREDENZIALI DI AUTENTICAZIONE: codice utente e password richieste dal sistema o dalla postazione di lavoro per verificare se l'utente è autorizzato ad accedere e con quali modalità.
- WHITE LIST: elenco di siti che l'Ente ritiene comunemente attinenti all'attività lavorativa.
- BLACK LIST: elenco di siti che presentano contenuti non attinenti all'attività lavorativa e, per questa ragione, sottoposti a filtri che si attivano qualora l'utente cerchi di accedervi.
- TITOLARE DEL TRATTAMENTO: persona fisica, giuridica, pubblica amministrazione e qualsiasi altro ente, associazione ed organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza. (Art. 28, D. Lgs. 30 giugno 2003, n. 196). In tale contesto, Titolare del trattamento risulta essere……

- RESPONSABILE DEL TRATTAMENTO: persona fisica, giuridica, pubblica amministrazione e qualsiasi altro ente, associazione, od organismo designati facoltativamente dal titolare al trattamento dei dati personali. (Art. 29 D. Lgs. 30 giugno 2003, n. 196). In tale contesto, Responsabile del trattamento risulta essere ……..
- INCARICATO: persona fisica autorizzata dal titolare o dal responsabile a compiere operazioni di trattamento di dati personali. (Art. 30 D. Lgs. 30 giugno 2003, n. 196).

3. UTILIZZO DELLA RETE E DEL PERSONAL COMPUTER

Le unità di rete sono aree di condivisione di dati ed informazioni strettamente legati all'attività lavorativa; pertanto i file ivi dislocati devono avere attinenza con attività e finalità di carattere istituzionale.
Ogni utente è responsabile per il proprio account e per l'uso che ne viene fatto, essendo tenuto a tutelarlo da accessi non autorizzati. Non è ammessa la comunicazione del proprio account a terzi.
Le disposizioni di seguito riportate, relative alle credenziali di autenticazione, contribuiranno a garantire la sicurezza nell'accesso:

- Scegliere una password composta da almeno 8 caratteri alfanumerici, che non contenga riferimenti che riconducano agevolmente all'incaricato (es: non inserire nome o cognome proprio e di familiari).
- La password è personale, riservata e non può essere ceduta o comunicata ad alcuno. E' pertanto vietato l'uso della password di altri utenti; qualora se ne venisse a conoscenza è obbligatorio segnalare il fatto all'utente interessato e al proprio responsabile.
- E' obbligatorio modificare la password ogni volta che il sistema ne faccia richiesta o, almeno, regolarmente ogni tre mesi.
- Per esigenze operative o di sicurezza e integrità del sistema e dei dati, l'Amministratore di sistema ha facoltà di modificare la password degli utenti.

Qualsiasi attività svolta utilizzando un codice utente e la relativa password sarà ricondotta nella sfera di responsabilità dell'utente assegnatario del codice. L'utente è civilmente responsabile di ogni danno cagionato all'Ente, all'Internet Provider e/o a terzi, non solo in relazione ai propri fatti illeciti ma anche per quelli commessi da chiunque utilizzi il suo codice utente e password.
La violazione delle presenti disposizioni può comportare l'applicazione di sanzioni disciplinari, rimanendo ferma ogni ulteriore forma di responsabilità penale.
Per evitare il pericolo di introdurre virus informatici o di alterare la stabilità delle applicazioni è vietato scaricare ed installare programmi, salva espressa autorizzazione da parte dell'Amministratore di sistema o del Responsabile nominato.
Non è consentito modificare le configurazioni del proprio PC.
Non è consentito scaricare file contenuti in supporti magnetici/ottici non aventi alcuna attinenza con la propria prestazione lavorativa.
Qualora un utente dovesse riscontrare malfunzionamenti, guasti o situazioni di rischio per la sicurezza o l'integrità del sistema causati da comportamento doloso o comunque non conforme alle istruzioni e disposizioni, deve darne immediata comunicazione al proprio responsabile e/o all'Amministratore di Sistema.

Il responsabile si riserva la facoltà di procedere alla rimozione di ogni applicazione o file ritenuti pericolosi per la sicurezza del sistema, non attinenti all'attività lavorativa o acquisiti ed installati in violazione del presente disciplinare.

4. UTILIZZO DI PC PORTATILI

L'utente al quale venga assegnato il PC portatile, ne è responsabile e dovrà custodirlo con la dovuta diligenza. In caso di utilizzo all'esterno dell'Ente, i PC dovranno essere custoditi in luogo sicuro.
Al PC portatile si applicano le regole sopra indicate per i PC connessi in rete, con particolare attenzione alle disposizioni concernenti i profili di accesso (password).
Sull'hard disk devono essere conservati solo i file strettamente necessari all'attività lavorativa, rimuovendo comunque, prima della restituzione del PC, quelli elaborati ed ivi salvati.
Collegarsi periodicamente alla rete interna per consentire gli aggiornamenti dell'antivirus, del sistema operativo, nonché la sincronizzazione della posta elettronica e relative cartelle pubbliche.
Non utilizzare abbonamenti Internet privati per collegarsi alla rete.

5. UTILIZZO DELLA RETE INTERNET

L'accesso ad Internet può essere effettuato da qualsiasi utente che sia autenticato (credenziali di accesso) su una qualsiasi postazione di lavoro connessa. Il lavoratore deve ricordare che Internet è uno strumento di lavoro e quindi è possibile che il datore, per ridurre i casi di utilizzo improprio del mezzo (es: visione di siti non correlati all'attività lavorativa, download di file e software, uso della rete per finalità completamente estranee alla propria mansione…), adotti misure che evitano un controllo a posteriori dei lavoratori.
Fra queste misure si possono enumerare: individuazione di *white list* (composte da soli "siti istituzionali, rispetto ai quali la navigazione è correlata e funzionale allo svolgimento della prestazione lavorativa) o *black list* (composte da tutti quei siti che, oltre a non avere attinenza con il lavoro, presentano contenuti – violenza, pornografia.. – che attivano filtri predisposti dall'Amministratore di sistema; se durante la navigazione si cerca di accedere ad un sito positivo ai filtri, l'utente viene avvertito con un messaggio e non sarà possibile visualizzare la pagina) e trattamento dei dati inerenti alla navigazione in forma anonima o in modo tale da precludere l'immediata identificazione del soggetto, ma tale da individuare l'anomalia nell'utilizzo degli strumenti informatici.
L'Ente ha adottato un sistema di prevenzione basato su una *black list*, aggiornata e modificata a cura dell'Amministratore di sistema. Qualora un utente cerchi di accedere ad una pagina web indicata nella *black list*, il filtro predisposto negherà l'accesso. È auspicabile che gli uffici dell'Ente segnalino le modifiche ritenute necessarie alla *black list* anche ai fini dell'attività istituzionale (es: sito bloccato da filtri che avrebbe un'utilità lavorativa).
L'utente è direttamente responsabile dell'uso che egli faccia del servizio di accesso ad Internet, dei siti ai quali accede, delle informazioni che immette e riceve, tanto durante lo svolgimento delle proprie mansioni sia nella fascia oraria a disposizione per la navigazione privata. Non è comunque consentito usare la rete in modo

difforme da quanto previsto dal presente disciplinare, dalle leggi penali, civili ed amministrative in materia.

6. UTILIZZO DELLA POSTA ELETTRONICA

Il sistema di posta elettronica attivato sulla rete dell'Ente è da intendersi strumento di lavoro e come tale deve essere utilizzato.

Se viene assegnato un *account* di posta elettronica ad ogni utente della rete informatica, l'accesso al contenuto della quale è protetto dalla richiesta di autenticazione; se viene creato un account condiviso fra più lavoratori che operano nel medesimo ufficio (es: info@…); in quest'ultimo caso risulta chiara la natura non privata dello strumento e della relativa corrispondenza.

Le disposizioni di seguito riportate sono enucleate al fine di garantire un corretto utilizzo dello strumento:

- All'utente non è consentito servirsi dell'account fornito dall'Ente per l'invio di mail non connesse con l'attività professionale (es: mail a contenuto privato, giochi, appelli, petizioni, catene di S. Antonio…).
- Non è consigliato allegare al testo delle comunicazioni, materiale potenzialmente insicuro o file di dimensioni eccessive. In quest' ultimo caso utilizzare formati compressi (zip, rar…)
- Nel caso di mittenti sconosciuti o di messaggi dall'oggetto insolito, è consigliata l'eliminazione senza l'apertura del messaggio. Lo stesso vale nel caso di messaggi provenienti da mittenti conosciuti che tuttavia presentano allegati con particolari estensioni (es: .exe, .scr, .pif., .bat..).
- Nel caso in cui si debba inviare un documento all'esterno, è preferibile utilizzare un formato protetto da scrittura (es: Acrobat).
- E' consigliabile non inviare mail che contengano dati sensibili; qualora ciò sia necessario per determinate esigenze, questi devono essere inviati comunicando al richiedente un codice identificativo per ogni soggetto e trasmettendo separatamente il documento privo del nominativo dell'interessato e crittografando i file con password che dovrà essere comunicata al destinatario del messaggio per altro mezzo.
- Qualora il messaggio debba essere inviato a più soggetti, gli indirizzi vanno inseriti solo nel campo "CCn" per tutelare la riservatezza dei medesimi, che ricevono il messaggio conoscendo solamente il mittente.
- Prevedere, in caso di assenza prolungata del lavoratore (es: ferie), l'invio di messaggi di risposta automatica che indichino la durata dell'assenza ed il nominativo del soggetto al quale è possibile rivolgersi. Se l'assenza risulta imprevista (es: malattia), l'attivazione dell'invio di messaggi automatici potrà essere richiesta dal responsabile all'Amministratore di sistema.
- L'iscrizione a mailing list è concessa solo per motivi professionali: prima di iscriversi è necessario verificare l'affidabilità del sito ed ottenere l'autorizzazione dell' Amministratore di sistema.
- L'intestatario dell'account ha facoltà di delegare ad altri il diritto d'accesso in caso di assenza prolungata e per garantire la continuità nell'attività lavorativa.

Il fiduciario dovrà essere scelto e nominato fra i colleghi o i collaboratori che, qualora dovessero accedere alla casella di posta della persona assente, sono tenuti a non aprire o non considerare i messaggi che presentino contenuto non attinente alle motivazioni per cui si effettua l'accesso.

L'Amministratore di sistema o chi da esso incaricato può avere accesso all'account solo ed esclusivamente a seguito del riscontro di situazioni che abbiano pregiudicato il funzionamento del sistema.

Il paragrafo 9 del presente regolamento disciplina i profili connessi ai controlli e alle eventuali sanzioni in cui si può incorrere qualora si utilizzi tale strumento in modo difforme.

7. INTERRUZIONE D'UFFICIO DEL SERVIZIO

L'Amministratore di sistema può sospendere temporaneamente il servizio di accesso ad Internet e alla posta elettronica in caso di manutenzione; l'interruzione sarà anticipatamente comunicata agli utenti, salvo casi di forza maggiore.

L'utilizzo del servizio di accesso alla Rete e all'account di posta elettronica cesserà d'ufficio nei seguenti casi:

- Qualora venga meno la condizione di dipendente o collaboratore munito di autorizzazione o se l'autorizzazione non fosse riconfermata.
- Se venga accertato un uso non corretto del servizio da parte dell'utente o estraneo ai suoi compiti professionali.
- In caso di manomissioni e/o interventi su hardware/software; diffusione o comunicazione imputabili direttamente o indirettamente all'utente relativamente a profili d'accesso o altre informazioni tecniche riservate; accesso a directory/file/siti non rientranti fra quelli per cui l'utente abbia autorizzazione;
- In caso di violazione o inadempimento imputabile all'utente rispetto a quanto stabilito nei precedenti punti; in ogni altro caso in cui sussista in modo evidente una violazione degli obblighi.

8. UTILIZZO DEL TELEFONO

Il telefono è uno strumento di lavoro e come tale deve esser utilizzato, per fini istituzionali.

Eventuali telefonate a carattere privato potranno essere effettuate con moderazione ed in casi di necessità.

9. CONTROLLI E SANZIONI DISCIPLINARI

Sono interdetti al datore di lavoro controlli del personale dipendente e dei collaboratori effettuati in maniera diretta, prolungata, costante o indiscriminata (art. 4, Statuto dei lavoratori, l. 300/1970).

Ciò premesso, l'Ente può avvalersi di sistemi controllo relativi al corretto utilizzo degli strumenti lavorativi che consentono indirettamente un controllo a distanza dell'effettivo adempimento della prestazione: tali controlli saranno effettuati qualora le misure minime preventivamente esposte non siano state sufficienti per evitare comportamenti anomali.

I controlli saranno svolti con gradualità, secondo i principi di pertinenza e non eccedenza.
In seguito si espongono le modalità di tali controlli:

- In prima battuta si effettuerà un controllo preliminare su dati anonimi ed aggregati; si procederà pertanto con verifiche di reparto, ufficio o gruppo di lavoro, in modo da individuare l'area da richiamare all'osservanza delle regole.
- Il controllo anonimo effettuato su aree può terminare con un avviso di rilevazione di un utilizzo inadeguato degli strumenti aziendali; contestualmente si diramerà una nota di richiamo invitando ad attenersi ai compiti e alle mansioni impartite.
- Se si dovesse ripetere l'anomalia, sarà facoltà dell'Ente procedere con controlli più mirati, anche su base individuale e successivamente procedere all'irrogazione di sanzioni disciplinari previste dall'art. 7 dello Statuto dei lavoratori (l. 300/1970) e dal contratto di assunzione. Il provvedimento disciplinare nei confronti del dipendente/collaboratore responsabile dell'anomalia, sarà comunque adottato solo dopo contestazione per iscritto dell'addebito e dopo aver sentito la difesa dell'interessato. Il provvedimento disciplinare sarà applicato dopo che siano trascorsi cinque giorni dalla contestazione del fatto che vi ha dato causa: entro tale termine il lavoratore destinatario potrà presentare le proprie giustificazioni in maniera sia verbale che scritta.
- La sanzione irrogata sarà proporzionata all'infrazione e potrà consistere in un biasimo scritto, in una multa, nella sospensione dal servizio e dalla retribuzione o addirittura nel licenziamento.

I dati contenuti nei file di log, relativi agli accessi ad Internet e al traffico telematico, sono conservati per il tempo strettamente necessario al perseguimento di finalità organizzative, produttive e di sicurezza.
I file di log potranno essere utilizzati in tali casi:

- Produzione di report statistici che presentino i dati relativi alla navigazione in forma aggregata e anonima.
- Per l'analisi dei problemi riscontrati nel sistema e soluzione dei medesimi, estraendo i dati in modo aggregato e in forma anonima
- Imputazione delle telefonate

Per ogni chiarimento sarà possibile rivolgersi a GALVAGNI RENZO, nominato Responsabile interno del trattamento, relativamente ai controlli ammessi in merito all'utilizzo della rete Internet e della posta elettronica.

IL TITOLARE DEL TRATTAMENTO: