PROVINCIA AUTONOMA DI TRENTO

Reg.delib.n. **1037** Prot. n.

VERBALE DI DELIBERAZIONE DELLA GIUNTA PROVINCIALE

O G G E T T O:
Utilizzo della rete internet, della posta elettronica, delle attrezzature informatiche e telefoniche - Approvazione Disciplinare.

Il giorno **07 Maggio 2010** ad ore **10:05** nella sala delle Sedute
in seguito a convocazione disposta con avviso agli assessori, si è riunita

LA GIUNTA PROVINCIALE

sotto la presidenza del

	PRESIDENTE	**LORENZO DELLAI**
Presenti:	VICE PRESIDENTE	**ALBERTO PACHER**
	ASSESSORI	**MAURO GILMOZZI**
		LIA GIOVANAZZI BELTRAMI
		TIZIANO MELLARINI
		ALESSANDRO OLIVI
		UGO ROSSI
Assenti:		**MARTA DALMASO**
		FRANCO PANIZZA
Assiste:	LA DIRIGENTE	**PATRIZIA GENTILE**

Il Presidente, constatato il numero legale degli intervenuti, dichiara aperta la seduta

Il Relatore comunica:

L'art. 46 bis della l.p. n. 7/1997, come introdotto dall'art. 23, c. 8 della l.p. n. 4/2009, dispone che per assicurare la funzionalità, la sicurezza e il corretto impiego degli strumenti informatici e delle reti telematiche da parte degli utilizzatori, la Giunta provinciale adotti, con proprio provvedimento, un disciplinare che definisca le misure di tipo organizzativo e tecnologico e individui le condotte e le forme di controllo ammissibili.

Con tale norma, diretta al perseguimento degli interessi generali cui l'organizzazione e l'azione amministrativa sono indirizzate (art. 36, c. 1, l.p. n. 7/1997 e s.m.), il legislatore provinciale prende atto di come l'uso delle tecnologie informatiche implichi notevoli rischi sia dal punto di vista della sicurezza nei luoghi di lavoro che di quello della funzionalità e del corretto impiego delle reti telematiche e degli strumenti informatici, fatti oggetto di specifiche previsioni in sede penale e fonti di possibile responsabilità dell'Amministrazione, con conseguente necessità, peraltro prevista dalle stesse fonti normative in svariati settori (contrasto al terrorismo, reati pedopornografici, illeciti finanziari e così via), di adottare le opportune misure volte a limitare e contenere i rischi predetti.

Tali misure si traducono nella necessaria adozione di strumenti di filtraggio e monitoraggio delle comunicazioni tali da consentirne il tracciamento tecnologico cui può potenzialmente accompagnarsi la possibilità di controllo indiretto della attività dei lavoratori. A salvaguardia dei diritti del lavoratore e, *in primis*, del diritto alla dignità e riservatezza, opera dunque un complesso normativo richiamato dall'art. 46 bis cit., ossia:

- il d.lgs. n. 82/2005 (Codice dell'amministrazione digitale), con particolare riferimento all'art. 2, c. 5 che riconosce il diritto dei cittadini a che il trattamento dei dati effettuato mediante l'uso di tecnologie telematiche sia conformato al rispetto dei diritti e delle libertà fondamentali, nonché alla dignità dell'interessato;
- il d.lgs. n. 196/2003 (Codice in materia di protezione dei dati personali), che sancisce il diritto alla protezione dei dati personali e dispone che ogni trattamento garantisca un elevato livello di tutela delle persone, nonché dei principi di semplificazione, armonizzazione ed efficacia (artt. 1 e 2); il legislatore prescrive, inoltre, che i trattamenti di dati siano effettuati per finalità determinate, esplicite e legittime, oltre a dover rispondere al principio di necessità e correttezza: ogni dato trattato in violazione della disciplina in materia non può essere utilizzato (artt. 11, 3);
- la l. n. 300/1970 (Statuto dei Lavoratori), con particolare richiamo all'art. 4 che, nel contemperamento tra le esigenze del datore di lavoro e quelle dei dipendenti, svolge a tutt'oggi un ruolo fondamentale, vietando da un lato il controllo diretto dei lavoratori e, dall'altro, ammettendo per esigenze organizzative produttive ovvero di sicurezza del lavoro, l'installazione di impianti e apparecchiature di controllo dalle quali possa anche derivare un controllo a distanza dell'attività dei lavoratori (c.d. controllo preterintenzionale). Nel settore privato si prevede per tali casi non la determinazione unilaterale del datore di lavoro ma il previo accordo con le OO.SS. o, in mancanza, l'autorizzazione dell'Ispettorato del lavoro.

Recentemente, anche l'Amministrazione statale, con la direttiva n. 2/2009 avente ad oggetto "Utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro", ha fornito indicazioni utili a facilitare, nell'ambito del settore pubblico, da un lato il corretto utilizzo degli strumenti ICT (postazioni di lavoro, connessioni di rete e posta elettronica) e, dall'altro il proporzionato esercizio del potere datoriale di controllo da parte delle Amministrazioni pubbliche.

Specifica rilevanza assume poi in materia la deliberazione n. 13/2007 del Garante per la protezione dei dati personali, che prescrive ai datori di lavoro alcune misure, necessarie o opportune, per conformare alle disposizioni vigenti il trattamento di dati personali effettuato per verificare il corretto utilizzo nel rapporto di lavoro della posta elettronica e di internet.

In particolare, il Garante, alla luce della normativa sopra richiamata, evidenzia la necessità che i trattamenti di dati si uniformino al principio di necessità e di correttezza e che siano sempre effettuati per finalità determinate, esplicite e legittime; sottolinea, inoltre, a tutela della libertà e dignità dei lavoratori, il divieto di installare apparecchiature preordinate al controllo a distanza dei dipendenti, ammettendo invece l'utilizzo di programmi e tecnologie che consentono indirettamente un controllo a distanza (c.d. controllo preterintenzionale), a condizione che ciò sia necessario per esigenze produttive o organizzative o, comunque, quando sia necessario per la sicurezza sul lavoro; evidenzia ancora come eventuali controlli sull'utilizzo degli strumenti informatici debbano ispirarsi al principio di pertinenza e non eccedenza, nell'equo bilanciamento di interessi tra le parti coinvolte.

Sono poi fortemente sottolineati dal Garante gli accorgimenti tecnici volti a prevenire comportamenti del lavoratore pericolosi per la sicurezza aziendale, di cui viene data ampia esemplificazione.

Il disciplinare per l'utilizzo della rete internet, della posta elettronica, delle attrezzature informatiche e telefoniche, di cui si propone l'approvazione, è dunque volto a garantire, in ossequio a quanto previsto dal legislatore, la sicurezza nei luoghi di lavoro, assicurare la funzionalità e il corretto impiego delle reti telematiche e degli strumenti informatici e di comunicazione, fermo restando il divieto di utilizzo di sistemi hardware e software esclusivamente preordinati al controllo a distanza dell'attività lavorativa del dipendente.

A tal fine il documento raccoglie, innanzitutto, una serie di elementari prescrizioni per il corretto utilizzo degli strumenti di lavoro (per es.: verificare l'assenza di virus dei supporti magnetici in input; mantenere la segretezza delle password; non lasciare incustodito e accessibile il PC durante la sessione di lavoro e così via). Il Disciplinare ribadisce poi il generale divieto, per i dipendenti provinciali, di utilizzare per ragioni personali Internet, la posta elettronica e le attrezzature informatiche; in deroga e solo al di fuori dell'orario di lavoro, consente, previa autorizzazione del dirigente, di avvalersi dei servizi Internet e di posta elettronica per motivi personali, nelle fasce orarie dalle 07.45 alle 09.00, dalle 12.45 alle 14.30 e dopo le 18.30 (prima e/o dopo l'orario di lavoro, per il personale a part-time orizzontale). Il Disciplinare regolamenta anche i controlli previsti per verificare il generale rispetto delle norme organizzative e di sicurezza. Tali controlli si svolgono, in prima istanza, in forma anonima (anche a campione) e, solo in caso di reiterazione o nei casi espressamente indicati (per gli illeciti civili, penali e amministrativi), in forma specifica e mirata, ossia mediante identificazione del singolo dipendente. Le verifiche possono riguardare anche il corretto utilizzo delle linee telefoniche

dell'ufficio: in deroga al generale divieto di effettuare telefonate personali, sono ammesse brevi e limitate chiamate tra il personale provinciale e, solo in casi eccezionali e urgenti, verso soggetti esterni. Il Disciplinare indica, inoltre, le misure di garanzia di tipo organizzativo e tecnologico che l'Amministrazione adotta, attraverso le strutture competenti, per assicurare il perseguimento delle predette finalità prevedendo, ad esempio: l'ubicazione dei server in luogo protetto, la periodica sostituzione della password su richiesta del sistema; l'individuazione di categorie di siti considerati non correlati con la prestazione lavorative (black list) e così via.

Il Disciplinare vieta, ovviamente, i controlli esclusivamente diretti all'attività del lavoratore nonchè, salvo diversa previsione dei contratti collettivi, l'utilizzo dei sistemi e dei dati al fine della valutazione quantitativa e qualitativa della prestazione del lavoratore nonché ai fini dell'accertamento del rispetto degli obblighi di comportamento del lavoratore nell'esecuzione del contratto di lavoro estranei all'ambito di regolazione del disciplinare e sempre che tale comportamento non costituisca più grave illecito civile, penale o amministrativo. Non è inoltre previsto l'utilizzo di software di controllo.

Il Disciplinare, in coerenza con le finalità perseguite, si applica non solo ai dipendenti provinciali ma anche, in quanto compatibile, agli altri soggetti che a vario titolo prestano servizio o attività per conto e nelle strutture della Provincia; costituisce inoltre linea guida per il corretto utilizzo tecnico delle strumentazioni informatiche per coloro che, a qualunque titolo, utilizzano il sistema informativo provinciale; infine, si rivolge anche agli enti pubblici strumentali della Provincia, fatta salva la possibilità di adottare un proprio disciplinare.

L'inosservanza delle prescrizioni in esso contenute può comportare, oltre all'irrogazione di sanzioni disciplinari nei confronti dei dipendenti, la sospensione o la revoca dell'autorizzazione ad accedere ai sistemi.

Sullo schema di Disciplinare sono state raccolte e recepite le osservazioni del Servizio semplificazione e sistemi informativi, del Servizio Reti e telecomunicazioni e del Servizio Edilizia pubblica e logistica.

Lo schema di Disciplinare è stato altresì comunicato alle Organizzazioni sindacali per eventuali osservazioni. Ha riscontrato la sola FENALT con nota d.d. 3 marzo 2010. Sulla base delle relative osservazioni si è innanzitutto meglio precisato all'art. 1 il divieto di controllo a distanza laddove esclusivamente diretto all'attività del dipendente, vietato dall'art. 4, c. 1, l. n. 300/1970; all'art. 12.2 lett. m) si è poi subordinato l'accesso del dirigente alla casella di posta elettronica del dipendente assente a improrogabili ragioni di ufficio.

La FENALT rileva inoltre che la recente sentenza della Corte di Cassazione n. 4375 del 23 febbraio 2010 stabilisce che i controlli a distanza preterintenzionali (funzionali a esigenze organizzative, produttive o di sicurezza) ricadono nell'art. 4, c. 2, l. n. 300/1970, che ammette il controllo a distanza solo in presenza di accordo sindacale, con il quale ultimo, dunque, non deve essere confuso il presente Disciplinare, restando l'accordo con le RSA presupposto imprescindibile di eventuali controlli.

Il punto merita specifica attenzione, dovendosi osservare come:

1) il Disciplinare ribadisce il divieto di controllo diretto dei lavoratori;
2) il Disciplinare presuppone l'utilizzo dei dati coessenziali al funzionamento dello strumento di lavoro (e non di controllo)

utilizzato dallo stesso lavoratore (per es. sistema operativo) e non già di software applicativi di controllo a tutela di esigenze produttive, organizzative o di sicurezza del lavoro muniti della concreta potenzialità, attraverso opportuni algoritmi di elaborazione dei predetti dati, di monitorare a distanza l'attività lavorativa individuale dei lavoratori, di rappresentarne cioè il minuto svolgimento e consentirne dunque, in modo meccanico, continuo e anelastico (come descritto nella Relazione Ministeriale all'art. 4), la precisa analisi critico-valutativa di conformità della prestazione resa alla prestazione attesa (micropause, assenze temporanee; ritmi di lavoro, errori operativi, modalità esecutive e così via: situazione questa efficacemente descritta con la locuzione "lavoratore di vetro"); di qui, secondo taluni orientamenti, la radicale estraneità, in difetto di previsione di tali strumenti, all'art. 4, l. n. 300/1970;

3) a prescindere da quanto sopra, la sentenza citata, appunto relativa ad un contesto aziendale ove era stato adottato un apposito software di controllo (Super Scout), non reca in ogni caso, nella materia, particolari novità rispetto alla precedente giurisprudenza, subordinando ad accordo "*i controlli diretti ad accertare comportamenti illeciti dei lavoratori*, quando *tali comportamenti riguardino l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro e non la tutela di beni estranei al rapporto stesso"*. L'accordo è dunque richiesto solo laddove il controllo consenta la verifica del diligente adempimento della prestazione lavorativa sotto il profilo quali-quantitativo e dell'osservanza delle connesse norme aziendali, restando invece estranei alla necessità dell'accordo i controlli "difensivi" diretti a prevenire e reprimere gli ulteriori illeciti civili nonchè gli illeciti penali e amministrativi posti a presidio di beni estranei all'ambito del diligente adempimento della prestazione;
4) anche a voler ulteriormente prescindere, l'art. 46-*bis*, l.p. n. 7/1997, norma diretta al perseguimento degli interessi generali cui l'organizzazione e l'azione amministrativa sono indirizzate (art. 36, c. 1, l.p. n. 7/1997 e s.m.), rimette il disciplinare a "provvedimento" della Giunta provinciale e non ad accordo con le RSA, sul punto derogando dunque alla norma comune di cui all'art. 4, c. 2, l. n. 300/1970.

Per migliore chiarezza, in linea con quanto sopra osservato sub n. 3) si è in ogni caso provveduto ad integrare lo schema di Disciplinare (art. 10, lett. E) e 18, lett. D)) con il già visto espresso divieto – salvo diversa previsione dei contratti collettivi - di utilizzo dei sistemi e dei dati ai fini della valutazione quantitativa e qualitativa della prestazione del lavoratore nonchè ai fini dell'accertamento del rispetto degli obblighi di comportamento del lavoratore nell'esecuzione del contratto di lavoro estranei all'ambito di regolazione del disciplinare e sempre che il comportamento non costituisca diverso illecito civile, penale o amministrativo.

L'entrata in vigore dell'allegato Disciplinare è fissata per il Capo I il giorno successivo al relativo invio per posta elettronica ai dipendenti e, per il

Capo II, il quindicesimo giorno successivo a quello di approvazione della presente delibera.

Tutto ciò premesso

LA GIUNTA PROVINCIALE

- udita la relazione,
- visto l'art. 46 *bis* della l.p. n. 7/1997,
- vista la precitata normativa nazionale,
- vista la deliberazione del Garante per la protezione dei dati personali e la citata direttiva,
- a voti unanimi espressi nelle forme di legge,

delibera

1. di approvare il Disciplinare per l'utilizzo della rete internet, della posta elettronica, delle attrezzature informatiche e telefoniche, allegato alla presente deliberazione quale parte integrante e sostanziale della stessa;
2. di dare atto che il Disciplinare è pubblicato sul sito Web della Provincia autonoma di Trento ed entra in vigore nel Capo I il giorno successivo al relativo invio per posta elettronica ai dipendenti e, nel Capo II, il quindicesimo giorno successivo a quello di approvazione della presente delibera;.
3. di disporre la pubblicazione del Disciplinare nel sito Web della Provincia autonoma di Trento.

AM - SD

Allegato parte integrante
Disciplinare per l'utilizzo della rete internet, della posta elettronica, delle attrezzature informatiche e telefoniche

DISCIPLINARE

PER L'UTILIZZO DELLA RETE INTERNET, DELLA POSTA ELETTRONICA, DELLE ATTREZZATURE INFORMATICHE E TELEFONICHE

Indice

CAPO I – INTERNET, POSTA ELETTRONICA E ATTREZZATURE INFORMATICHE

Titolo I
Oggetto, presupposti generali, destinatari e definizioni

1. Oggetto

Il presente Disciplinare, adottato con provvedimento della Giunta della Provincia autonoma di Trento in adempimento di quanto previsto dall'art. 46 bis l.p. n. 7/1997, nel rispetto di quanto previsto dal decreto legislativo 7 marzo 2005, n. 82 (Codice dell'amministrazione digitale), del decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali) e della legge 20 maggio 1970, n. 300 (Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento) nonché secondo le indicazioni contenute nella deliberazione 1° marzo 2007 nr. 13 del Garante per la protezione dei dati personali, recante "Linee guida del Garante per posta elettronica e internet", ha per oggetto **i criteri e le modalità operative di accesso e utilizzo del servizio internet, di posta elettronica, delle attrezzature informatiche e telefoniche,** al fine di garantire la disponibilità e l'integrità dei propri sistemi informativi e di comunicazione nonché la sicurezza sul lavoro.

A tal fine la PAT adotta, nel rispetto delle libertà fondamentali e della dignità dei lavoratori, idonee misure di sicurezza e organizzative, fermo restando il divieto di utilizzo di sistemi hardware e software preordinati al solo fine del controllo a distanza dell'attività lavorativa del dipendente, in particolare, con i seguenti mezzi:

- lettura e registrazione dei messaggi di posta elettronica/telefonici dei dipendenti ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per fornire il servizio di posta elettronica e telefonico;
- riproduzione ed eventuale memorizzazione delle pagine web visualizzate dal dipendente;
- lettura e registrazione dei caratteri inseriti dai lavoratori tramite la tastiera ovvero dispositivi analoghi a quello descritto;
- analisi occulta dei dispositivi per l'accesso a internet o l'uso della posta elettronica e dei telefoni messi a disposizione dei dipendenti.

2. Rischi per la disponibilità e integrità dei sistemi informativi, telefonici e delle attrezzature informatiche

L'utilizzo delle strumentazioni informatiche da parte del dipendente, implica in particolare l'esposizione alle seguenti fonti di rischio alla cui prevenzione sono dirette le citate misure di sicurezza:

- l'utilizzo di una connessione ad Internet (ad esempio via modem) a mezzo di un *provider* diverso da Informatica Trentina in assenza della protezione garantita da un *firewall,* pone in pericolo il PC utilizzato e l'intera rete provinciale;
- le operazioni non consentite in reti e siti terzi, l'accesso a siti impropri e lo scaricamento di file non autorizzati possono essere illegali e puniti dalla legge penale, oltre che essere fonte di responsabilità patrimoniale dell'Amministrazione;
- l'utilizzo della connessione Internet della Provincia per finalità estranee all'attività di lavoro può essere causa di sovraccarico della linea e riflettersi nel deterioramento della velocità della connessione per tutti gli utenti;
- le informazioni presenti su siti Internet non connessi a istituzioni ben conosciute possono essere non accurate, non valide o deliberatamente false, dal che la necessità di valutare adeguatamente le decisioni sulle stesse fondate;

- i messaggi di posta elettronica, di cui sia sconosciuto il mittente debbono essere trattati con le dovute cautele essendo essi la maggiore causa di eventi dannosi per virus informatico all'interno delle reti aziendali;
- i servizi che hanno un costo diretto rapportato all'effettivo utilizzo devono essere monitorati e utilizzati nei limiti delle esigenze di servizio .

3. Destinatari

Il Disciplinare si applica:

a) ai dipendenti della Provincia autonoma di Trento dell'area non dirigenziale del comparto autonomie locali;
b) ai dirigenti e direttori provinciali, nei limiti indicati;
c) al personale ATA del comparto del personale della scuola;
d) agli altri soggetti che a vario titolo prestano servizio o attività per conto e nelle strutture della Provincia (es.: *lavoratori socialmente utili, collaboratori, tirocinanti e stagisti*), in quanto compatibile;
e) infine, i contenuti del presente disciplinare costituiscono inoltre, per tutti coloro che, a qualunque titolo, utilizzano il sistema informativo provinciale, linee guida per il corretto utilizzo tecnico delle strumentazioni informatiche.

Il presente Disciplinare si applica inoltre, in quanto compatibile, fatta salva la possibilità di adottare un proprio disciplinare che regoli la materia, anche nei confronti degli Enti pubblici strumentali della Provincia autonoma di Trento.
Per comodità, si indicherà indistintamente con il termine di dipendente/utente, il soggetto autorizzato dall'Ente ad utilizzare le risorse informatiche, le attrezzature informatiche e i telefoni.
Il presente Disciplinare costituisce inoltre, nella parte relativa alla rete internet, linea guida di corretto utilizzo per i Comuni aderenti al SIEP.

4. Definizioni

Nel presente documento si intende per:

- ACCOUNT: costituisce quell'insieme di funzionalità, strumenti e contenuti attribuiti ad un utente in determinati contesti operativi. In informatica, attraverso il meccanismo dell'account, il sistema mette a disposizione dell'utente un ambiente con contenuti e funzionalità personalizzabili, oltre ad un conveniente grado di isolamento dalle altre utenze parallele;
- DOWNLOAD: trasferire programmi o dati da un'unità connessa al proprio computer ad un personal computer;
- BACK UP: copia di sicurezza o copia di riserva, indica l' operazione tesa a duplicare su differenti supporti di memoria le informazioni (dati o programmi) presenti sui dischi di stazione di lavoro, o di un server. Normalmente viene svolta con una periodicità stabilita;
- BYTE: è l'unità elementare di memorizzazione composta da 8 bit . Di solito un byte rappresenta un singolo carattere, come un numero, una lettera o un simbolo;
- BLACK LIST: elenco di siti non accessibili da nessun utente;
- BLACKBARRY: connettività wireless (dall'inglese senza fili – sistemi di comunicazione tra dispositivi elettronici, che non fanno uso di cavi), che consente di restare collegati con i propri contatti anche quando si è lontani dall'ufficio;
- CLIENT: una componente che accede ai servizi o alle risorse di un'altra componente, detta server. In questo contesto si può quindi parlare di client riferendosi all'hardware o al software;
- CHIAVE USB (o penna USB, o pendrive): è una memoria di massa portatile di dimensioni molto contenute (qualche centimetro in lunghezza e intorno al centimetro in larghezza) che si collega al computer mediante la comune porta USB ;

- DIRECTORY: è una specifica entità del *file system* che elenca altre entità, tipicamente file e altre directory, e che permette di organizzarle in una struttura ad albero;
- FILE: un contenitore di informazione digitalizzata. Le informazioni codificate al suo interno sono leggibili solo da software;
- FIREWALL: apparato di rete hardware o software che filtra tutti i pacchetti entranti ed uscenti, da e verso una rete o un computer, applicando regole che contribuiscono alla sicurezza della stessa;
- FLOPPY DISK: supporto di memorizzazione che contiene all'interno di un contenitore quadrato o rettangolare di plastica un disco sottile e flessibile (in inglese "floppy") su cui vengono memorizzati magneticamente i dati;
- GPRS: (General Packet Radio Service): è uno standard per comunicazioni cellulari che consente trasmissioni fino a 150 Kb al secondo. Rappresenta una soluzione particolarmente adatta alla spedizione e ricezione di posta elettronica o alla navigazione web con terminali cellulari;
- HARD DISK: tipologia di dispositivo di memoria di massa che utilizza uno o più dischi magnetici per l'archiviazione dei dati;
- HARDWARE: parte fisica del computer, ovvero di tutte quelle parti magnetiche, ottiche, meccaniche ed elettroniche che lo compongono;
- HOSTING: designa il servizio di gestione di un sito Web ospitato su un elaboratore aziendale;
- INPUT: insieme di elementi in entrata, per realizzare o produrre qualcosa;
- INTERNET PROVIDER : l'Azienda che fornisce alla PAT il canale di accesso ad Internet;
- IP: un Indirizzo IP è un numero che identifica univocamente un dispositivo collegato a una rete informatica che comunica utlizzando lo standard IP(protocollo informatico), ossia un protocollo di rete a pacchetto, non connesso;
- LOG: registrazione cronologica delle operazioni e il file su cui tali registrazioni sono memorizzate;
- MAIL-LIST: lista di utenti interessati allo scambio di informazioni su un argomento comune, utilizzando la posta elettronica;
- OUTPUT: Informazioni o segnali provenienti dal computer e diretti verso una periferica esterna ad esso; l'output consiste generalmente in dati stampati su carta, visualizzati sul monitor;
- PEER TO PEER: si intende una rete di computer o qualsiasi rete informatica che non possiede nodi gerarchizzati come client o server fissi (clienti e serventi), ma un numero di nodi equivalenti (in inglese peer) che fungono sia da cliente che da servente verso altri nodi della rete;
- PORTA : è una connessione attraverso cui vengono mandati e ricevuti dati;
- PROXY: programma che si interpone tra un client ed un server, inoltrando le richieste e le risposte dall'uno all'altro;
- RESET: ripristino delle situazioni iniziali di un sistema di elaborazione;
- ROAMING: il roaming (*Rintracciabilità nel territorio*), identifica nelle reti telematiche e di telecomunicazione un insieme di normative e di apparecchiature che permettono di mettere in comunicazione due o più reti distinte. Il roaming viene utilizzato dagli operatori telefonici di telefonia cellulare per permettere agli utenti di collegarsi utilizzando una rete non di loro proprietà. Ciò può accadere quando l'utente si trova all'estero e l'operatore telefonico non ha una rete propria, oppure quando l'utente si trova nel paese di origine dell'operatore telefonico ma questo non ha una copertura totale della nazione, (in questo caso l'operatore si appoggia sulle reti telefoniche di altri operatori). Attraverso il roaming, quindi, l'operatore consente all'utente la possibilità di utilizzare il servizio in tutta la nazione.
- RINGING: suono della chiamata del telefono, in attesa di risposta.

- SCREEN SAVER: è un'applicazione per computer che provoca l'oscuramento dello schermo o la comparsa di un'animazione o di una serie di immagini in successione sullo stesso dopo un periodo programmato di inattività del mouse e della tastiera (non dell'elaboratore in sé), impostabile attraverso un timer;
- SERVER: designa il o i computer utilizzati dalla PAT per fornire i servizi previsti;
- SOFTPHONE: in informatica un softphone è un programma software per effettuare chiamate telefoniche su internet utilizzando un computer di uso generale, piuttosto che utilizzare hardware dedicato. Spesso un softphone è stato progettato per comportarsi come un telefono tradizionale, a volte appare come l'immagine di un telefono cellulare, con un pannello del display e pulsanti con i quali l'utente può interagire. Un softphone di solito è usato con un auricolare collegato alla scheda audio del PC, o con un telefono USB.
- SOFTWARE: termine generico che indica l'insieme dei programmi che permettono di far eseguire al computer specifiche istruzioni;
- UMTS: Terza generazione di trasmissione di testo, voce, video, multimedia e dati a banda larga basata sulla trasmissione a pacchetti. Il trasferimento dei dati avviene ad una velocità di 2 megabits al secondo e si basa sullo standard GSM Global System for Mobile;
- WAP: Wireless Application Protocol. Tecnologia per il collegamento di telefoni cellulari a sistemi di posta elettronica o a siti Internet appositamente realizzati (solo testo);
- WEB: un insieme vastissimo di contenuti multimediali, e di servizi, di Internet, contenuti e servizi che possono essere resi disponibili dagli stessi utenti di Internet;
- WHITE LIST: elenco di siti direttamente e immediatamente accessibili da tutti gli utenti internet.

Titolo II
Internet, posta elettronica e attrezzature informatiche

5. Utilizzo della rete Internet

Nell'ambito dell'accesso al servizio Internet, è in ogni caso vietato:

a) salvo quanto previsto al punto 8, utilizzare i servizi di rete per ragioni personali estranee all'attività di servizio. E' invece liberamente consentito l'accesso al sito ufficiale della PAT ed alla rete Intranet;
b) consentire ad altri di servirsi della stazione di accesso ad Internet per attività non istituzionali.

6. Utilizzo della posta elettronica

Nell'ambito dell'accesso al servizio di posta elettronica, è in ogni caso vietato:

a) salvo quanto previsto al punto 8, l'utilizzo della posta elettronica per ragioni personali estranee al servizio. In particolare, il dipendente non può fornire l'indirizzo della propria casella di posta elettronica al fine di ricevere corrispondenza non di servizio, né spedire corrispondenza non di servizio.
   In deroga al sopra indicato divieto, la posta elettronica può essere utilizzata in orario di servizio:
   - esclusivamente per brevi e ridotte comunicazioni di carattere personale fra dipendenti stessi;
   - per comunicazioni non di servizio rivolte a soggetti esterni, a condizione che queste ultime abbiano oggettivo carattere di eccezionalità ed urgenza;

b) è altresì fatto divieto di utilizzare la casella di posta elettronica per partecipare a dibattiti, forum o mail-list non attinenti la propria attività o funzione svolta per l'Ente, salvo diversa ed esplicita autorizzazione;
c) per i servizi di posta elettronica, in caso di assenza programmata il lavoratore deve utilizzare apposita funzionalità automatica del sistema di invio di avviso al mittente dell'assenza del destinatario, con contestuale indicazione di altro eventuale referente della struttura di appartenenza, con relativo indirizzo e-mail e/o telefonico, per eventuali urgenze.

7. Utilizzo delle attrezzature informatiche e trattamento dati

A) Ai fini della presente regolamentazione, per attrezzature informatiche si intendono tutti i personal computer, sia fissi che portatili e tutte le periferiche connesse (come ad esempio, scanner, unità aggiuntive di memoria, palmari, blackbarry) escluse le stampanti.
Salvo quanto previsto al punto 8, ogni utilizzo delle attrezzature informatiche per finalità estranee all'attività di servizio è vietato.

B) In ogni caso, nell'uso delle attrezzature informatiche:

a) è obbligatorio, nell'utilizzo dei supporti magnetici in input verificare l'assenza di virus, ove questo sia tecnicamente possibile, prima di procedere all'elaborazione di dati;
b) è obbligatorio, prima della consegna a terzi, procedere alla cancellazione delle informazioni precedentemente contenute per esempio in floppy disk, cd-rom riscrivibili, chiave USB e hard disk;
c) è vietato utilizzare, per la conservazione di dati la cui sicurezza vada garantita, le unità logiche/dischi (CD, dischi fissi o locali) installati fisicamente sul PC in luogo delle unità di rete (Server);
d) è vietato l'utilizzo, salvo autorizzazione dell'amministratore di sistema, di password di file;
e) è vietato l'accesso, al personale non autorizzato, ai locali in cui sono custoditi i server;
f) è necessario garantire presso la postazione di lavoro, nel caso di interventi di manutenzione sulla macchina e/o di assistenza, la presenza dell'utente o del referente informatico o, in loro assenza, di altro dipendente della struttura individuato dal responsabile della medesima;
g) il personale assegnatario di PC portatili li utilizza esclusivamente per gli scopi cui sono diretti; evita di lasciare incustodito il PC, di connettersi, salvo necessità di servizio, a reti diverse da quella provinciale, assicurando in ogni caso, in accordo con la struttura competente, l'adeguata protezione antivirus. Provvede al backup dei dati connettendosi al server dell'ufficio o, se impossibile, su supporti magnetici adeguatamente custoditi;
h) è vietato ogni tipo di modifica (aggiunta, rimozione, sostituzione) dei componenti interni delle apparecchiature informatiche, essendo tali operazioni di competenza esclusiva del Servizio preposto;
i) nessun utente è autorizzato ad installare sulle apparecchiature informatiche software diversi da quelli compresi nella dotazione base o a modificarne la configurazione, senza il preventivo consenso dell'amministratore di sistema;
j) l'utente è responsabile delle attrezzature che gli sono affidate in uso e, pertanto, deve provvedere a mantenerle in completa efficienza segnalando tempestivamente al Servizio preposto ogni eventuale problema tecnico ed eventuali dubbi sulla sicurezza della postazione di lavoro;
k) in caso di furto o smarrimento di attrezzature, l'utente è tenuto a segnalare immediatamente l'accaduto al proprio dirigente, che provvederà alla denuncia presso l'autorità competente. In tali evenienze il lavoratore dovrà dare comunicazione anche al Servizio preposto.

C) Nel trattamento di dati con strumenti elettronici il lavoratore deve:

a) adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in proprio possesso ed uso esclusivo (divieto di rendere note a più persone le password e di condividerle). E' in primo luogo interesse dell'utente evitare che altri utilizzino la sua password d'accesso; infatti, dalla registrazione dell'attività effettuata dal sistema, risulterebbe a lui attribuito il trattamento effettuato da altri con connessa responsabilità in caso di trattamenti scorretti o non autorizzati o illeciti. Il dipendente deve, in particolare, evitare di trascrivere le password su supporti facilmente accessibili a terzi;
b) non lasciare incustodito e accessibile lo strumento elettronico durante la sessione di lavoro;
c) rispettare le modalità previste per la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento;
d) rispettare i divieti, gli obblighi e le prescrizioni disposte in materia dall' Amministrazione.

8. Criteri e modalità di utilizzo personale di Internet, della posta elettronica e delle attrezzature informatiche

A) In deroga ai predetti divieti, è ammesso, nei limiti di cui ai successivi punti e di quanto disposto dalle disposizioni contrattuali, l'utilizzo personale dei servizi di Internet e di posta elettronica nonché delle attrezzature informatiche (esclusa la stampa), di cui al precedente punto n. 7 lett. A), come segue:

a) per i dirigenti, senza pregiudizio per l'attività di servizio;
b) per i direttori, solo al di fuori dell'orario di lavoro, senza pregiudizio per l'attività di servizio;
c) per il restante personale, limitatamente ai soli servizi di Internet e posta elettronica, solo al di fuori dell'orario di lavoro, senza pregiudizio per le esigenze organizzative, secondo le disposizioni impartite dal Dirigente e negli orari dallo stesso indicati nell'ambito delle seguenti fasce temporali:
   - per i dipendenti a tempo pieno e a part-time verticale - dalle ore 07.45 alle 09.00; dalle ore 12.45 alle 14.30; dopo le ore 18.30 ;
   - per i dipendenti a part-time orizzontale – prima e/o dopo l'orario di lavoro.

Quanto sopra, anche al fine di consentire ai dipendenti di assolvere incombenze amministrative e burocratiche senza allontanarsi dai luoghi di lavoro (ad esempio, per effettuare adempimenti on line nei confronti di pubbliche amministrazioni e di concessionari di pubblici servizi), in linea con quanto prevede la Direttiva nr. 02/09 dd. 26.05.2009 del Ministro per la Pubblica amministrazione e l'Innovazione: limitatamente a tali operazioni è consentita, in deroga al vigente divieto, la stampa dei documenti strettamente necessari.

Nell'ambito di specifici progetti, debitamente formalizzati, volti ad armonizzare il diritto al lavoro con altri diritti costituzionalmente tutelati (ad esempio conciliazione lavoro – famiglia), la struttura competente in materia di personale può motivatamente consentire l'utilizzo personale dei servizi di Internet e di posta elettronica nonché delle attrezzature informatiche in orario di lavoro precisandone contenuti e limiti.

B) L' utilizzo personale di Internet, della posta elettronica e, laddove consentito, delle attrezzature informatiche deve avvenire in conformità ai seguenti principi:

a) assenza di aggravio diretto di spesa per l'Amministrazione;
b) assenza di interferenza con i tempi di lavoro condivisi con colleghi e collaboratori;
c) assenza delle attività non consentite, di cui al successivo punto C);
d) puntuale rispetto delle disposizioni sulla sicurezza e la protezione dei dati personali, di cui al presente disciplinare;

e) nell'uso della casella di posta elettronica assegnata dall'Amministrazione, adozione di ogni cautela volta ad evitare un uso implicito del nome della Provincia Autonoma di Trento in contesti diversi da quelli strettamente ufficiali.

C) Nell'ambito dell'uso personale dei servizi e, laddove consentito, delle attrezzature informatiche, non sono comunque consentite le attività che interferiscono con l'efficienza e le funzionalità dei sistemi informatici e dei servizi di rete.

E' in particolare vietato/a:

a) scaricare (download) da Internet file estranei all'attività di servizio (es.: file audio o video), di dimensioni tali da interferire con l'efficienza dei servizi di rete o condivisione degli stessi attraverso sistemi di tipo peer to peer; in deroga a tale divieto è ammesso lo scarico di file di dimensioni ridotte, a condizione che ogni eventuale memorizzazione avvenga su supporti non di proprietà della PAT e in condizioni di massima sicurezza (cd rom; chiavetta USB, ecc.);
b) ogni attività anche non riconducibile al punto precedente che porti comunque alla violazione di diritti protetti dalle norme sulla proprietà intellettuale;
c) produrre siti Web, installare Web camera, operare servizio di Hosting, come anche la mera conservazione di tali file su supporti di proprietà della PAT;
d) l'utilizzo delle apparecchiature per lo svolgimento di attività extra-lavorative non autorizzabili, ai sensi della normativa sulle incompatibilità;
e) l'invio di messaggi con allegati di dimensione tale da compromettere la normale operatività della posta per l'inoltro di messaggi non sollecitati ("lettere a catena");
f) la trasmissione o ricezione deliberata di contenuti di tipo pornografico o di istigazione all'odio razziale e all'intolleranza politico-religiosa o comunque di carattere illecito;
g) ogni altra attività di carattere illecito.

Titolo III
Dati oggetto di trattamento, controlli, sanzioni e altre misure

9. Dati oggetto di trattamento e relativa conservazione

a) Le informazioni conservate relative al traffico internet (attraverso i log di sistema) sono le seguenti: data e ora dell'evento; IP sorgente; porta sorgente; IP di destinazione; porta di destinazione; durata della comunicazione; byte scambiati durante la comunicazione.
b) Le informazioni conservate relative al traffico di posta elettronica sono le seguenti: data e ora dell'evento; IP della postazione che ha generato l'evento; indirizzo di posta del mittente; indirizzo di posta del destinatario. I dati memorizzati sono conservati in forma anonima fatta eccezione per le informazioni desumibili dagli indirizzi di posta formulati nella classica forma "nome.cognome".
c) La conservazione dei dati di traffico internet e della posta elettronica avviene in maniera centralizzata presso la Società Informatica Trentina S.p.A., in linea con la convenzione vigente tra la stessa e la Provincia Autonoma di Trento.
d) Il periodo di conservazione delle informazioni relative al traffico telematico è, di norma, pari a 6 mesi, ai sensi dell'art. 132 del D.lgs. 196/2003.
e) La cancellazione delle informazioni telematiche avviene nel rispetto dei termini fissati dal comma 1 dell'art. 132 del D.lgs. 196/2003.
f) La gestione dei dati di traffico relativo ai dipendenti della Provincia, ivi compreso l'accesso, è interamente effettuata dalla società Informatica Trentina spa in linea con la convenzione vigente tra la stessa e la Provincia Autonoma di Trento.

10. Controlli

A) Nel rispetto delle predette prescrizioni l'Amministrazione si riserva di effettuare, per le citate finalità, i seguenti controlli:

1) **in forma anonima,** c.d controllo generale e routinario, anche a campione e automatico in modo da precludere l'identificazione degli utenti e/o delle loro attività, con cadenza periodica (di norma trimestrale).

I dati anonimi aggregati, riferibili all'intera struttura o sue aree, sono posti a disposizione dell'ufficio competente in materia disciplinare, per le valutazioni di competenza e riguardano i dati di cui al punto n. 9 e, in particolare:

- per ciascun sito/dominio visitato: il numero di utenti che lo visitano, il numero delle pagine richieste e la quantità di dati scaricati;
- per ciascun utente, presentato in forma anonima: il numero dei siti visitati, la durata del collegamento e la quantità totale dei dati scaricati.

In caso di rilevazione di comportamenti anomali non rientranti nelle fattispecie di cui al successivo punto n. 2), i dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia sono avvisati dell'accertato utilizzo improprio della rete Internet e contestualmente invitati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

2) **in forma non anonima,** c.d. controllo specifico e mirato , in relazione :

- al caso in cui l'integrità del sistema sia minata da un problema di sicurezza e sia indispensabile la consultazione dei file di log per individuare e eliminare l'anomalia;
- alla prevenzione e all'accertamento, in presenza di indizi, di illeciti civili, penali e amministrativi;
- all'indispensabilità dei dati di log rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- all'obbligo di rispondere ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria;
- al rispetto del vincolo di utilizzo fuori orario di lavoro di cui al precedente punto 8;
- al caso di persistente utilizzo anomalo degli strumenti da parte degli utenti di una specifica struttura/area (rilevabile esclusivamente dai dati aggregati), nonostante l'avviso a cessare tale comportamento di cui al precedente punto n. 1).

I controlli, alle condizioni descritte, potranno essere effettuati:

- sugli accessi ad Internet;
- sulla posta elettronica ricevuta ed inviata dal dipendente, considerato che la casella di posta assegnata dall'Amministrazione all'utente è uno strumento di lavoro, per cui la posta ricevuta e trasmessa non è in ogni caso da considerarsi corrispondenza privata;
- sul corretto utilizzo delle attrezzature informatiche;
- sulla singola postazione di lavoro con le modalità di cui alla successiva lett. B).

B) Il controllo sulla singola postazione di lavoro può essere esercitato, laddove necessario, anche attraverso ispezioni dirette dal responsabile dell'ufficio competente in materia disciplinare o suo delegato e condotte d'ufficio o su richiesta del dirigente della struttura di appartenenza del dipendente, eventualmente assistito dall' amministratore di sistema anche ai fini del reset della password e alla presenza dell'assegnatario del PC o suo delegato o, se impossibile, del responsabile della struttura. Dell'ispezione viene redatto verbale consegnato in copia all'interessato che può rendere nel medesimo, se presente, proprie osservazioni. Nel corso dell'ispezione il dipendente ha l'obbligo di osservare le istruzioni

impartite dal responsabile dell'ispezione medesima e di fornire la password per l' accesso al sistema.

C) Salvo quanto disposto al punto 8, le verifiche e le ispezioni sono condotte su motivata richiesta:
- del Presidente della Giunta provinciale, per i dirigenti;
- del Dirigente generale competente in materia di personale, per i direttori;
- del Dirigente della struttura di appartenenza o d'ufficio dal Dirigente competente in materia di personale, per i restanti dipendenti.

D) Laddove il controllo possa compromettere il segreto professionale cui il dipendente sia chiamato per specifica norma di legge, sulla relativa opposizione decide, assunta cognizione dell'oggetto, il segretario generale sentito il dirigente della struttura di assegnazione. Nel frattempo il controllo resta sospeso. Il Segretario generale dispone, ove necessario, le opportune misure cautelari.

E) Fermo restando quanto disposto dall'art. 1 e salvo diversa previsione dei contratti collettivi, è in ogni caso fatto divieto di utilizzo dei sistemi e dei dati indicati al punto n. 9 ai fini della valutazione quantitativa e qualitativa della prestazione del lavoratore nonché ai fini dell'accertamento del rispetto degli obblighi di comportamento del lavoratore nell'esecuzione del contratto di lavoro estranei all'ambito di regolazione del presente disciplinare e sempre che il comportamento non costituisca diverso illecito civile, penale o amministrativo.

11. Sanzioni e altre misure di tutela

a) Fermo restando quanto previsto dalla lett. E), l'accertato mancato rispetto dei predetti divieti, obblighi e prescrizioni è punito secondo quanto previsto dal Codice disciplinare, salve restando, in capo al dipendente, le ulteriori responsabilità in sede civile, penale e amministrativa.

b) L'utilizzo del servizio di accesso ad internet e della posta elettronica può essere sospeso o interrotto d'ufficio nei seguenti casi:
- qualora non sussista più la condizione di dipendente o collaboratore autorizzato o non fosse confermata l'autorizzazione all'uso;
- qualora venga accertato un uso non corretto del servizio da parte dell'utente o comunque un uso estraneo ai suoi compiti professionali;
- in caso di manomissioni e/o interventi sul hardware e/o sul software dell'utente impiegati per la connessione compiuti eventualmente da personale non autorizzato;
- in caso di diffusione o comunicazione, imputabili direttamente o indirettamente all'utente, di password, procedure di connessione, indirizzo IP ed altre informazioni tecniche riservate;
- in caso di accesso doloso dell'utente a directory, a siti e/o file e/o servizi da chiunque resi disponibili non rientranti fra quelli autorizzati e in ogni caso qualora l'attività dell'utente comporti danno, anche solo potenziale al sito contattato;
- in ogni altro caso in cui sussistano ragionevoli evidenze di una violazione degli obblighi dell'utente.

Titolo IV
Misure di garanzia

12. Premessa

Al fine di assicurare, nel perseguimento delle predette finalità, la funzionalità, la sicurezza e il corretto impiego degli strumenti informatici e delle reti telematiche da parte degli utilizzatori, l'Amministrazione, attraverso le strutture competenti, garantisce le seguenti misure organizzative e tecnologiche.

12.1 Misure organizzative

a) Si procede alla sistematica valutazione degli effetti sui diritti dei lavoratori prodotti dall'introduzione e applicazione di nuove misure volte a salvaguardare la sicurezza ed il mantenimento dell'efficienza dei sistemi.
b) Individuazione (anche tipologica) dei lavoratori cui è accordato l'utilizzo della posta elettronica e internet. L'assegnazione al dipendente delle dotazioni strumentali d'ufficio, ivi compresi i diversi applicativi quali internet, posta elettronica, banche dati, software specialistici, nonché le relative abilitazioni, è richiesta, in riferimento alle mansioni svolte dal dipendente, dal responsabile della struttura di appartenenza.
c) Ubicazione dei server in apposite stanze a ciò destinate o in armadi chiusi muniti di serratura e/o altre protezioni adeguate con relativa individuazione dell'incaricato alla custodia .
d) Accessibilità delle postazioni di lavoro solo da quanti ne hanno titolo, in qualità di responsabili o incaricati del trattamento, di amministratori del sistema o altro, nei soli limiti in cui ciò sia funzionale allo svolgimento dei compiti della struttura o per lo svolgimento di attività di manutenzione, di pulizia e affini, nonché per altre attività comunque indispensabili.
e) Accesso fisico ai luoghi di lavoro protetto tramite la presenza di personale di portineria ovvero tramite la chiusura delle vie di accesso, sempre nel rispetto delle norme antincendio.
f) Presidio del personale di portineria degli uffici aperti al pubblico; negli orari diversi da quelli di servizio, ove non vi sia comunque un presidio, la porta di accesso all'edificio deve rimanere chiusa.
g) Presenza di personale abilitato quale "amministratore di sistema" a sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e a consentirne l'utilizzazione. Tale personale può vedere e modificare le cartelle e i dati di tutti gli utenti collegati al server e consentire a terzi autorizzati l'accesso. Ciò attraverso il reset della password del dipendente (quale solo strumento, questo, di protezione da accessi estranei all'Amministrazione). In caso di assenza dell'incaricato al trattamento che non sia raggiungibile e di urgenza di accesso ai dati, ivi compresa la posta elettronica, l'amministratore, su richiesta scritta e motivata del dirigente responsabile, consente l'accesso ai dati. Dell'avvenuto accesso è data comunicazione al dipendente. L' amministratore di sistema è destinatario di corsi di formazione, organizzati periodicamente dall'amministrazione, sulla gestione e sulla sicurezza delle reti, sui principi di protezione dei dati personali e sul segreto delle comunicazioni.
h) L'Amministrazione impegna Informatica Trentina (IT), quale responsabile del trattamento dei dati, in piena conformità alla normativa vigente ivi comprese le presenti disposizioni, a garantire, in particolare, il segreto sugli atti e le informazioni di cui la stessa venga a conoscenza, ad adottare le misure necessarie ad assicurare che i controlli avvengano nei limiti sopra definiti nonché a ridurre le operazioni di manutenzione allo stretto necessario.

12.2 Misure tecnologiche

Rispetto alla **navigazione Internet**

a) Protezione della rete TelPAT da firewall, gestito da Informatica Trentina .
b) L'accesso al PC e alla rete avviene attraverso l'utilizzo di un identificativo utente (user-id) e di una password.
c) Periodica sostituzione della password su richiesta del sistema.
d) Screen Saver vincolato e automatico protetto da password con tempo di attivazione inferiore a 5 minuti di inattività del PC.
e) Individuazione di categorie di siti considerati correlati (white list) o non correlati (black list) con la prestazione lavorativa.
f) Previsione di sistemi o di filtri volti a prevenire determinate operazioni vietate: attualmente è attivo un sistema di "url filtering" ovvero un sistema per il monitoraggio del traffico web che permette di bloccare la navigazione verso i siti non consentiti, contenenti materiale per adulti o riconducibili a pratiche illecite.
g) Possibilità di attivare, su richiesta di ogni singolo responsabile di struttura, l'applicazione di specifiche politiche più o meno restrittive – rispetto a quelle indicate sopra al punto f) - in considerazione dell'attività svolta e delle tematiche trattate dai diversi utenti .
h) Trattamento delle registrazioni in forma anonima o tale da precludere l'immediata identificazione degli utenti mediante opportune aggregazioni.
i) In caso di conservazione delle registrazioni, limitazione al tempo strettamente necessario al perseguimento delle finalità organizzative, produttive e di sicurezza, attraverso procedure di cancellazione periodica automatica (sovraregistrazione) dei dati personali relativi agli accessi ad Internet e al traffico telematico, salvo i casi di particolari esigenze di sicurezza, difesa in sede giudiziaria, giustizia.
j) I controlli sui comportamenti anomali, esclusi in ogni caso quelli prolungati, costanti ed indiscriminati, devono essere graduati: di primo livello, in via preliminare, su dati aggregati, riferiti all'intera struttura e/o area/servizio, con avvisi generali che informano dell'accertato utilizzo improprio della rete Internet e contestuale invito ad attenersi scrupolosamente ai compiti assegnati e istruzioni impartite. L'avviso potrà essere circoscritto ai dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia; di secondo livello effettuati invece su base individuale, laddove specificatamente necessario per la tutela dell'Amministrazione, anche in sede giudiziaria o nelle altre sedi competenti. Resta fermo quanto previsto dall'art. 10.

Rispetto alla **posta elettronica**

k) Eventuale attivazione di caselle c.d. "di struttura", ossia esercizi di posta condivisi che permettono sia la ricezione che l'inoltro della posta a soggetti diversi purché preventivamente e adeguatamente autorizzati .
l) Invito a tutti gli utenti di configurare dal proprio client di posta elettronica – secondo le relative indicazioni – nel caso di assenza programmata, un messaggio di risposta automatica, che indichi i riferimenti elettronici e/o telefonici di altro referente dell'ufficio e/o struttura di appartenenza.
m) Possibilità da parte del responsabile del trattamento (Dirigente), qualora si presenti la necessità, per improrogabili ragioni di ufficio, di accedere a dati contenuti in una casella di posta elettronica e l'incaricato (titolare della casella) abilitato all'accesso a tale cartella sia irreperibile, di chiedere che il proprio account e/o quello di altri incaricati siano abilitati all'accesso a tale casella.
n) Possibilità da parte degli utenti di Lotus Notes di delegare uno o più colleghi per la lettura della propria posta, secondo le indicazioni fornite allo scopo.

o) Inserimento di un messaggio di avvertimento ai destinatari della posta elettronica sulla natura non riservata della corrispondenza e sulla possibilità che la risposta sia letta da altri.
p) I controlli sui comportamenti anomali, sono graduati su due livelli: quelli di primo livello avvengono in forma anonima, in forma c.d. aggregata (riferibili all' intera struttura e/o area), con avvisi generali che informano dell'accertato utilizzo improprio della posta elettronica, rivolti al solo personale assegnato alla struttura/area sottoposta a verifica; i controlli di secondo livello sono effettuati invece su base individuale, laddove specificatamente necessario per la tutela dell'Amministrazione, anche in sede giudiziaria o nelle altre sedi competenti. Resta fermo quanto previsto dall'art. 10.

CAPO II – SERVIZI TELEFONICI

Titolo I
Regole comportamentali nell'utilizzo dei telefoni fissi, mobili e personali

13. Uso dei telefoni fissi – Regole di buon utilizzo

A) Divieti di utilizzo personale e relative deroghe

I dipendenti non utilizzano le linee telefoniche dell'ufficio e i mezzi di comunicazione vocale assimilabili (es.: softphone per effettuare chiamate tramite PC; sistemi di videochiamata/videoconferenza) per effettuare telefonate personali. Durante l'orario di lavoro, la ricezione di telefonate personali sulle linee telefoniche dell'ufficio è limitata al minimo indispensabile.

In deroga a quanto sopra, sono ammesse brevi e limitate comunicazioni telefoniche personali:

- tra il personale provinciale;
- verso soggetti esterni, solo in caso eccezionali e urgenti.

Nell'ambito di specifici progetti, debitamente formalizzati, volti ad armonizzare il diritto al lavoro con altri diritti costituzionalmente tutelati (ad esempio conciliazione lavoro – famiglia), la struttura competente in materia di personale può motivatamente consentire l'utilizzo personale dei telefoni fissi e dei mezzi di comunicazione assimilabili precisandone contenuti e limiti.

B) Deviazioni

In caso di assenza e laddove l'apparecchio già non sia così configurato in via automatica, è opportuno deviare il proprio numero interno sull'apparecchio della Segreteria o di un collega, secondo le modalità puntualmente indicate nell'elenco telefonico interno.

C) Risposta per assente

Nel caso di assenza o comunque di impossibilità a rispondere, il collega d'ufficio che occupa la medesima stanza riceve le telefonate del collega, secondo le istruzioni indicate nell'elenco telefonico interno.

D) Segnalazione guasti

La segnalazione di eventuali guasti deve avvenire quanto prima, agli indirizzi forniti dall'Amministrazione.

14. Uso dei cellulari aziendali

A) Utilizzo individuale e collettivo

Al fine di evitare l'improprio utilizzo di apparecchi di telefonia mobile (con relativa "sim card") dell'Amministrazione, si evidenzia che il consegnatario del cellulare di servizio è il responsabile del corretto utilizzo del medesimo. Nel caso in cui un apparecchio sia concesso a più utilizzatori, il consegnatario è individuato nel Dirigente o responsabile della struttura o, suo delegato. In tal caso la struttura dovrà tenere nota degli effettivi utilizzatori per tutta la durata della concessione.

In ogni caso, al fine di ridurre il possibile uso fraudolento in caso di furto o smarrimento, il dipendente deve sempre attivare la richiesta del codice personale di identificazione (PIN) all'accensione del terminale.

B) Uso privato del cellulare aziendale

L'uso a fini personali delle apparecchiature (con le limitazioni sottoesposte) può avvenire solo in caso di contratto di billing (doppia fatturazione), anteponendo il codice che permette di addebitare i costi per l'uso privato sul conto corrente personale del titolare dell'utenza.

Per quanto riguarda le limitazioni all'impiego privato del cellulare aziendale, si rimanda alle dettagliate circolari del Servizio competente (Servizio Reti e Telecomunicazioni).

E' vietato in ogni caso l'invio dei cosiddetti SMS solidali (per le donazioni) e degli SMS premium con i quali è possibile sottoscrivere un abbonamento ad un servizio che, a sua volta, prevede l'invio periodico e automatico di messaggi a pagamento contenenti suonerie, oroscopo, ecc.

C) Blocco utenza cellulare

In caso di furto o smarrimento degli apparati e schede sim, occorre immediatamente bloccare l'utenza chiamando i numeri forniti dall'Amministrazione e, quindi, presentare denunzia alle autorità di pubblica sicurezza indicando il numero telefonico ed il codice IMEI dell'apparecchio (visibile sotto la batteria oppure digitando sul cellulare *#06#). La denuncia deve essere consegnata al Servizio Reti e Telecomunicazioni per il reintegro dell'apparecchio e della SIM.

15. Uso del cellulare privato

E' consentito un moderato utilizzo del cellulare privato (o di quello dell'Amministrazione a doppia fatturazione) in orario di servizio, limitatamente a comunicazioni brevi e strettamente necessarie.

Titolo II
Dati oggetto di trattamento, controlli, sanzioni e altre misure di tutela nell'utilizzo di telefoni fissi o mobili

16. Monitoraggio dei dati telefonici – Finalità

Al fine di monitorare e contenere i costi telefonici, la PAT installerà un sistema di documentazione (centralina elettronica) che renda possibile l'accorpamento delle linee esterne.

17. Conservazione dei dati telefonici

La conservazione dei dati, nell'ambito del sistema di documentazione di cui sopra (centralina telefonica) avviene per il periodo di tempo strettamente necessario, in ogni caso non superiore a 24 mesi, da parte della società Trentino Network; gli stessi dati sono trattati da parte di un numero strettamente necessario di addetti, debitamente autorizzati e quindi vincolati ad obbligo di riservatezza.

Sono conservati i dati relativi al traffico telefonico uscente da ciascun apparato, escludendo le ultime tre cifre della selezione effettuata da ogni singolo utente, ai fini della tutela della privacy.

I fornitori dei servizi telefonici conservano i dati di traffico telefonico, compresi quelli relativi alle chiamate senza risposta, necessari ad individuare :

numero dell'interno chiamante; numero di rete pubblica chiamato; ora di composizione chiamata; ora di risposta alla chiamata; ora di chiusura chiamata; durata complessiva della chiamata, compreso ringing; durata della chiamata da fatturare, traffico voce, eventuale trasferimento ad altro interno durante la chiamata o se è chiamata semplice.

Il trattamento dei dati relativi al traffico strettamente necessario ai fini di fatturazione per l'abbonato è consentito al fornitore del servizio telefonico per un periodo non superiore a sei mesi.
Per finalità di accertamento e repressione dei reati, i citati dati sono invece conservati dal fornitore per 24 mesi dalla data di comunicazione.
Ai sensi dell'art. 124 del D.lgs. 196/2003, nella fatturazione dell'abbonato non sono evidenziate le ultime tre cifre dei numeri chiamati. Ad esclusivi fini di specifica contestazione dell'esattezza di addebiti determinati o riferiti a periodi limitati, l'abbonato può richiedere la comunicazione dei numeri completi delle comunicazioni in questione.

18. Controlli sui dati telefonici

A) I controlli sui dati telefonici possono essere:

a) in forma anonima, anche a campione e automatici, sui telefoni fissi: il Dirigente competente trasmette ai Dirigenti dei Servizi interessati i dati relativi al superamento per ogni bimestre della percentuale massima di tolleranza, c.d. "soglia"; il personale assegnato ai/l Servizio/i coinvolto/i sarà genericamente richiamato dal Dirigente di riferimento - anche a mezzo e-mail - al corretto utilizzo del telefono, nel rispetto delle disposizioni del vigente disciplinare;
si precisa che sono equiparati al trattamento dei dati in forma anonima anche i dati di ogni singola utenza ma aggregati per direttrice (es.: SMS, roaming internazionali, off net, ecc.) non evidenziati in tabulati analitici;

b) in forma non anonima "c.d. controllo specifico e mirato" - sui telefoni fissi e sui cellulari di servizio, in base a tabulati analitici e in relazione:
   - al caso in cui l'integrità delle linee telefoniche sia minata da un problema di sicurezza;
   - alla prevenzione e all'accertamento, in presenza di indizi, di illeciti civili, penali e amministrativi;
   - a fatturazioni che laddove dettagliate – perché "sospette" - evidenzino un utilizzo improprio del cellulare di servizio (es.: loghi e suonerie; da concorsi e sondaggi, etc.); in questo caso l'identificazione dell'utente è coessenziale al controllo che, pertanto, sarà sempre e solo in forma non anonima;
   - all'indispensabilità dei dati di log rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
   - all'obbligo di rispondere ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria;
   - al caso di persistente utilizzo anomalo degli strumenti da parte degli utenti di una specifica struttura/area (rilevabile esclusivamente dai dati aggregati), nonostante l'avviso a cessare tale comportamento.

B) Tali controlli puntuali sono ammessi su motivata richiesta:

a) del Presidente della Giunta provinciale, per i dirigenti;
b) del Dirigente Generale competente in materia di personale, per i direttori;
c) del Dirigente della struttura di appartenenza o d'ufficio dal Dirigente competente in materia di personale, per i restanti dipendenti.

C) Laddove il controllo possa compromettere il segreto professionale cui il dipendente sia chiamato per specifica norma di legge, sulla relativa opposizione decide, assunta cognizione dell'oggetto, il segretario generale sentito il dirigente della struttura di assegnazione. Nel frattempo il controllo resta sospeso. Il Segretario generale dispone, ove necessario, le opportune misure cautelari.

D) Fermo restando quanto disposto dall'art. 1 e salvo diversa previsione dei contratti collettivi, è in ogni caso fatto divieto di utilizzo dei sistemi e dei dati indicati al punto n. 17 ai fini della valutazione quantitativa e qualitativa della prestazione del lavoratore nonché ai fini dell'accertamento del rispetto degli obblighi di comportamento del lavoratore nell'esecuzione del contratto di lavoro

estranei all'ambito di regolazione del presente disciplinare e sempre che il comportamento non costituisca diverso illecito civile, penale o amministrativo.

19. Sanzioni e altre misure di tutela

Fermo restando quanto previsto dalla lett. D), l'accertato mancato rispetto dei predetti divieti, obblighi e prescrizioni è punito secondo quanto previsto dal Codice disciplinare, salve restando, in capo al dipendente, le ulteriori responsabilità in sede civile, penale e amministrativa.

In ogni caso in cui sussistano ragionevoli evidenze di una violazione degli obblighi dell'utente, può essere disposta la sospensione o la revoca del servizio telefonico (fisso e/o mobile) ovvero può essere limitato il servizio di accesso alla rete telefonica.

CAPO III – DISPOSIZIONI FINALI

20. Pubblicità ed entrata in vigore

Il presente disciplinare è pubblicato sul sito Web della Provincia autonoma di Trento ed entra in vigore nel Capo I il giorno successivo al relativo invio per posta elettronica ai dipendenti e, nel Capo II, il quindicesimo giorno successivo a quello di approvazione.

21. Informativa ai lavoratori ai sensi dell'art. 13, D.lgs. n. 196/2003

Si rinvia in merito all'allegato A).

22. Ulteriori prescrizioni

I dirigenti dei Servizi rispettivamente competenti per le materie qui disciplinate, possono impartire, con proprie circolari opportunamente pubblicizzate, prescrizioni operative in merito ai contenuti del presente Disciplinare.

- Servizio per il Personale -

TRATTAMENTO DATI PERSONALI
RELATIVI ALL'UTILIZZO, DELLA RETE INTERNET, DELLA POSTA ELETTRONICA E STRUMENTI INFORMATICI

NOTA INFORMATIVA
AI SENSI DELL'ART. 13 DEL DECRETO LEGISLATIVO N. 196/2003

Con riferimento al Disciplinare relativo all'utilizzo della rete internet, della posta elettronica e degli strumenti informatici, La si informa che ogni trattamento dei Suoi dati personali avverrà nel rispetto delle seguenti disposizioni:

a) *Oggetto del trattamento* - informazioni relative al Suo utilizzo di Internet, della posta elettronica nonché degli strumenti informatici, comprensive di eventuali dati sensibili (opinioni religiose, filosofiche, politiche, stato di salute e vita sessuale).
b) *Finalità del trattamento* – verifica del corretto utilizzo di Internet, posta elettronica e degli strumenti informatici e telefonici a garanzia della disponibilità ed integrità dei sistemi informativi nonché della sicurezza sul lavoro.
c) *Modalità del trattamento* – informatizzato e manuale; effettuato da soggetti autorizzati all'assolvimento di tali compiti, edotti dei vincoli imposti dal decreto legislativo n. 196/2003 e con misure atte a garantire la riservatezza dei dati ed evitare l'accesso ai dati stessi da parte di soggetti terzi non autorizzati.
d) *Obbligatorietà del conferimento dati* – in quanto indispensabile per l'assolvimento degli obblighi di cui sopra; pertanto, l'opposizione al trattamento potrebbe comportare l'impossibilità di prosecuzione del rapporto.
e) E' Suo diritto (art. 9 , 2. n. D.lgs. 196/2003), anche mediante terza persona fisica, ente, associazione od organismo cui abbia conferito delega o procura, conoscere i dati che La riguardano ed intervenire circa il loro trattamento ai sensi di quanto previsto dall'articolo 7 del citato decreto legislativo.
f) Il TITOLARE del trattamento è la Provincia autonoma di Trento con sede in piazza Dante, 15 – 38122 Trento.
g) I RESPONSABILI per i trattamenti di dati personali relative alle materie di rispettiva competenza e alle funzioni di gestione amministrativa, finanziaria e tecnica sono:

- i dirigenti generali, laddove gestiscano a titolo esclusivo determinati trattamenti;
- i dirigenti, ivi compresi i dirigenti delle Agenzie comunque denominati;
- la Società "Informatica trentina Spa", responsabile (esterno) dei trattamenti della stessa effettuati ai fini della gestione del Sistema Informativo Elettronico Provinciale (S.I.E.P.);
- i gestori telefonici, tra i quali anche Trentino Network, per i dati telefonici.

h) INCARICATO del trattamento è la persona fisica autorizzata dal titolare a compiere le operazioni di trattamento di dati personali, attenendosi alle istruzioni impartite dal titolare e dal responsabile. La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito.