Provincia di Lecco

Regolamento per il corretto utilizzo degli strumenti informatici e telematici

APPROVATO CON DELIBERAZIONE DELLA G.P. N. 102 DEL 23/04/2009

Validità

La presente procedura è valida per tutta la rete dati della Provincia di Lecco.
Deve essere utilizzata anche per i processi in cui è necessario l'ausilio di dotazioni informatiche ovvero con l'utilizzo di software e in tutte le attività di manutenzione hardware e software.

Introduzione

La progressiva diffusione delle nuove tecnologie informatiche ed in particolare il libero accesso alla rete Internet dei Personal Computer, espone la Provincia di Lecco ai rischi di un coinvolgimento sia patrimoniale che penale, creando problemi alla sicurezza e all'immagine dell'Ente stesso.
Premesso quindi che l'utilizzo delle risorse informatiche e telematiche del nostro Ente deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, l'Amministrazione Provinciale di Lecco adotta il presente Regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.
Tali prescrizioni si aggiungono ed integrano le specifiche istruzioni già fornite a tutti gli incaricati in attuazione del D. Lgs. n. 196 del 30 giugno 2003 in materia di protezione dei dati personali.

Art. 1 Utilizzo del Personal Computer e delle periferiche connesse

1. Il Personal Computer affidato al dipendente è uno strumento di lavoro. Ogni utilizzo non attinente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Tutti gli strumenti citati sono di esclusiva proprietà dell'Ente, messi a disposizione del lavoratore al solo fine dello svolgimento delle proprie mansioni lavorative.
2. L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata. La stessa password è attivata per l'accesso alla rete.
3. Non è consentita l'attivazione della password di accensione (Bios).
4. Non è consentito installare autonomamente software, poichè sussiste il grave pericolo di propagare virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore. Tali programmi verranno automaticamente cancellati ed ogni violazione verrà automaticamente segnalata all'Ente.
5. Non è consentito l'uso di programmi diversi da quelli distribuiti ufficialmente dalla Provincia di Lecco (D. Lgs. 518/92 sulla tutela giuridica del software e L. 248/2000 e successive modifiche ed integrazioni recante nuove norme di tutela del diritto d'autore).
6. Non è consentita l'installazione sul personal computer in dotazione di alcun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, …).
7. E' vietato avviare applicativi da chiavetta USB o da qualunque altro supporto esterno, inclusi applicativi via web.
8. Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale del servizio CED nel caso in cui siano rilevati virus informatici.
9. Non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
10. Non è possibile spostare personal computer, stampanti ed ogni altro apparato informatico collegato direttamente o indirettamente alla rete, se non dopo averlo comunicato al Centro Elaborazione Dati ed all'Ufficio Economato.
11. Il Personal Computer, il monitor, le stampanti locali e di rete devono essere spente al termine dell'attività lavorativa prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. In ogni caso lasciare un elaboratore incustodito connesso alla rete può essere

causa di utilizzo da parte di terzi senza che vi sia la possibilità di provare in seguito l'indebito uso. In tali frangenti ogni responsabilità sarà addebitata al proprietario delle credenziali.

Art. 2 Utilizzo di dispositivi esterni di memorizzazione dati: chiavette usb, hard disk esterni, macchine fotografiche digitali, iPOD, lettori MP3, ecc.

1. E' vietato l'uso dei dispositivi esterni di memorizzazione su tutti i personal computer della rete, salvo diversa autorizzazione fatta dal Dirigente di Settore e comunicata mediante lettera al Dirigente del Settore Organizzazione e Gestione Risorse Umane. Le porte USB dei personal computer non autorizzate verranno disabilitate ove possibile. Viene comunque sconsigliato l'uso di tali dispositivi su postazioni con l'accesso da parte di utenti generici, stagisti, consulenti e su postazioni di front-office con servizi rivolti ai cittadini o ritenute strategiche al funzionamento dell'Ente.
2. E' vietato l'uso di dispositivi personali esterni all'Ente.
3. Il dispositivo di proprietà dell'Ente che risulta infetto da virus deve essere OBBLIGATORIAMENTE e TEMPESTIVAMENTE consegnato direttamente dall'utente al personale dell'Ufficio CED. Il responsabile del CED procederà alla segnalazione scritta per ogni virus rilevato sui dispositivi al Dirigente del Settore Organizzazione e Gestione Risorse Umane.
4. Il personale dell'ufficio CED, non essendo in grado di verificare l'attendibilità di tali supporti, non potrà procedere ad eventuali richieste di verifica presenza virus.
5. I supporti magnetici e digitali riutilizzabili (dischetti, cassette, chiavi USB …) contenenti dati personali devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato. Una persona esperta potrebbe, infatti, recuperare i dati memorizzati anche dopo la loro cancellazione. I supporti magnetici contenenti dati personali devono essere custoditi in archivi chiusi a chiave.
6. Non è consentito scaricare file contenuti in supporti magnetici/ottici (Hard Disk) non aventi alcuna attinenza con la propria prestazione lavorativa.
7. Eventuali danni derivanti dalla mancata osservanza del rispetto delle presenti norme saranno imputati al dipendente.

Art. 3 Particolari dispositivi esterni

1. E' vietato l'uso e/o l'installazione di software di collegamento/condivisione dati con i personal computer o portatili dei dispositivi, quali telefoni cellulari, navigatori satellitari, ecc.
2. E' altresì vietato il collegamento alla rete dati provinciale di dispositivi con connessioni di tipo Wireless, Bluetooth o di altra tipologia per scambio dati.

Art. 4 Utilizzo dei personal computer portatili

1. L'utente è responsabile del portatile assegnatogli che deve essere custodito con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
2. Ai portatili si applicano le regole di utilizzo previste per i personal computer connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.
3. E' vietato collegare in rete personal computer portatili non di proprietà dell'Ente (ad esempio consulenti, stagisti, ecc), salvo diversa esplicita autorizzazione scritta del Dirigente del Settore, da inoltrare al Dirigente del Settore Organizzazione e Gestione Risorse Umane.
4. E' vietato collegare nel dominio provinciale personal computer portatili. Non sarà dunque possibile configurare sul portatile utenze personali (ad esempio: nome.cognome), per

accedere alla rete provinciale, alle stampanti di rete, alle cartelle condivise ed ai programmi provinciali.

5. Al fine di evitare la ricezione ed eventuale successiva diffusione di virus informatici, i p.c. portatili appartenenti all'Ente non potranno essere collegati a reti esterne.
6. In ottemperanza al testo unico sulla privacy, tutti i personal computer portatili dell'Ente dovranno essere obbligatoriamente portati dagli utenti all'ufficio CED con cadenza periodica bimestrale al fine di provvedere ad aggiornare l'antivirus ed il sistema operativo.

Art. 5 Protezione antivirus

1. Il sistema di protezione contro virus informatici è monitorato dal Centro Elaborazione Dati. L'aggiornamento dell'antivirus sui PC connessi in rete avviene in modo automatico.
2. Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico mediante virus o mediante ogni altro software aggressivo.
3. Su segnalazione dei tecnici del Centro Elaborazione Dati, nel caso che il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer, al fine di permettere il completamento delle operazioni di bonifica.
4. Si raccomanda di porre particolare attenzione all'utilizzo di floppy disk, cd rom, chiavette USB e memorie di massa.

Art. 6 Uso della posta elettronica provinciale

1. La casella di posta, assegnata all'utente, è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse. E' fatto divieto di utilizzare le caselle di posta elettronica ***@provincia.lecco.it*** per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list non attinenti alla propria attività lavorativa, salvo diversa ed esplicita autorizzazione.
2. E' vietato inviare catene telematiche (o di Sant'Antonio). Se si ricevono messaggi di tale tipo, è necessario non attivare gli allegati di tali messaggi e non rispondere ad essi al fine di evitare danni alla rete provinciale.
3. E' buona norma evitare messaggi completamente estranei al rapporto di lavoro. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.
4. La dimensione massima delle caselle postali è limitata; superata tale quota viene automaticamente bloccata la casella di posta elettronica.
5. Gli allegati alle mail in ingresso ed in uscita non possono superare la dimensione di 10 MB.
6. Gli allegati devono rispettare le seguenti caratteristiche:
    a. Non possono contenere file Audio (Es. AIFF, MIDI, MPEG Sun/Next, WAW, CD, Ogg Vorbis Audio File, ASF, Windows Media File, …)
    b. Non possono contenere file Video (Es. AVI, DVM, MPEG; Quicktime, ShockWave File, Windows Media ASX File, ecc)
    c. Non possono contenere file eseguibili e file con "codici sorgente".
7. E' vietato l'uso di programmi e/o servizi (esterni) di posta elettronica anonima che permettono di impersonare terze persone nei messaggi inviati..
8. Le password di ingresso al sistema di mail mediante Web sono previste ed attribuite inizialmente dall'Amministratore del Sistema. E' consentita in ogni modo l'autonoma sostituzione da parte degli utenti.
9. E' vietato configurare account di posta elettronica diversi da quelli provinciali sul proprio personal computer.

Art. 7 Navigazione Internet e relativi servizi

1. Il personal computer abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. Non è permessa la navigazione in Internet e ogni forma di registrazione a siti per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.
2. E' fatto divieto all'utente scaricare e/o installare software e programmi, così pure scaricare musica, film, filmati e ogni altro file coperto da diritti d'autore.
3. E' tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni remote banking, attività di broking (brokeraggio) e trading, acquisti on-line e simili, salvo i casi direttamente autorizzati dal Dirigente e nel rispetto delle normali procedure di acquisto.
4. E' vietata la partecipazione a Forum non professionali, l'utilizzo di chat, di bacheche elettroniche e le registrazioni in guest book, anche utilizzando pseudonimi (o nicknames). E' vietata la partecipazione a social-network di qualunque natura (facebook, myspace, ..) nonché attività di dating online.
5. E' vietata la consultazione della posta elettronica privata e di qualunque altro riferimento estraneo al sistema di posta elettronica dell'Ente.

Art. 8 Controllo sull'utilizzo di internet e posta elettronica

1. Si rimanda all'Appendice al presente regolamento per quanto attiene alle modalità con le quali l'Ente potrà accertare e quindi reprimere le condotte illecite dei dipendenti utilizzatori di internet e della posta elettronica.

Art. 9 Utilizzo delle cartelle di rete

1. Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Su queste unità sono svolte regolari attività di controllo, amministrazione e backup da parte del Centro Elaborazione Dati.
2. E' fatto particolare divieto di salvare file (anche compressi) di formato:
   - Multimediale (aif, asf, au, avi, mid, midi, miv, mov, mp2, mp3, mp4, mpe, mpeg, mpg, qt, rmi, snd, wav, wm, wma, wmv, mp3a, mp3b, ogg, 3gp)
   - Eseguibili (exe, cmd, reg, vbs)
   - Posta elettronica (pst, pab, eml, msg, idx, mbx, mmf, dbx)
   - giochi, screen saver e comunque ogni file non attinenti all'attività lavorativa
   - immagini in formato BMP (tali immagini devono essere convertite in formato JPG, JPEG al fine di occupare il minor spazio possibile).
3. Ad ogni utente è attribuita su File Server una cartella personale e una di gruppo a cui possono accedere gli utenti del medesimo settore e/o servizio per la condivisione dei file, laddove se ne ravvisi la necessità. Il Dirigente di settore può accedere a tutte le cartelle del proprio settore.
4. Per motivi di sicurezza è vietato condividere in altro modo cartelle fra utenti sul proprio PC, poiché possono costituire delle minacce ai dati custoditi, oltre a non ottemperare alle disposizioni di cui al D. Lgs. n. 196/2003.
5. L'Amministratore del Sistema può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza della rete dati sia sui PC degli incaricati sia sulle unità di rete.
6. Costituisce buona regola la periodica pulizia degli archivi (almeno ogni sei mesi), con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. E', infatti, assolutamente da evitare un'archiviazione ridondante.
7. Non è consentita la modifica dei permessi di accesso delle cartelle di rete da parte degli utenti.

8. La lunghezza dei nomi dei file conservati sui server non deve superare i 50 caratteri. Il sistema di back up (salvataggio dati) in uso non è in grado di salvare file con nomi di lunghezza superiore.
9. E' sconsigliato, per motivi di performance e per evitare che temporanee interruzioni nel collegamento facciano perdere il lavoro, operare direttamente su Server. L'utente è invitato a lavorare sul disco del proprio PC e di trasferire il proprio lavoro su Server al fine di effettuare un salvataggio (o una copia).

Art. 10 Gestione delle Password

1. Le password d'ingresso alla rete ed ai programmi sono personali, segrete e vanno comunicate e gestite secondo le procedure di seguito delineate. E' assolutamente proibito entrare nella rete e nei programmi con altri nomi utente.
2. Le password di ingresso alla rete, di accesso ai programmi e dello screen saver, sono previste ed attribuite inizialmente dall'Amministratore del Sistema. Successivamente deve essere effettuata l'autonoma sostituzione delle stesse da parte degli incaricati al trattamento con contestuale comunicazione al Custode delle Copie delle Credenziali (Dirigente del Settore).
3. Le password utilizzate dagli incaricati al trattamento dei dati hanno durata massima di TRE MESI, trascorsi i quali devono essere sostituite.
4. La password devono avere le seguenti caratteristiche:
    - non deve avere nomi comuni
    - non deve contenere nomi di persona
    - deve contenere sia lettere che numeri
    - deve contenere almeno 3 caratteri alfabetici
    - deve contenere almeno 2 caratteri numerici
    - deve essere diversa dallo User-Id
    - deve essere lunga 8 caratteri o massimo consentito dal sistema di autenticazione
    - non deve essere riconducibile all'incaricato
5. La password deve essere immediatamente sostituita, dandone comunicazione al Custode delle Copie delle Credenziali, nel caso si sospetti che la stessa abbia perso la segretezza.
6. In caso di smarrimento della password di accesso, l'utente deve comunicarlo all'Amministratore del Sistema che procederà a fornire una password provvisoria. L'utente, una volta connesso in rete, dovrà sostituirla e dovrà comunicarla al proprio Custode delle Copie delle Credenziali.
7. In casi eccezionali l'Amministratore del Sistema è autorizzato alla sostituzione della password su richiesta dell'interessato, del Segretario Generale o del Dirigente per competenza.
8. Ogni settore/servizio è tenuto ad organizzarsi la tenuta del registro e la custodia delle credenziali.
9. Il personale tecnico, a fini inerenti l'attività lavorativa e su disposizione dell'Amministratore del Sistema, è tenuto alla richiesta della password all'utente interessato o al Custode delle Copie delle Credenziali, in sua assenza.
10. Gli utenti incaricati del trattamento dei dati non possono accedere contemporaneamente con lo stesso account da più PC.

Art. 11 Salvataggio dei dati (Backup)

1. L'utente è responsabile dei dati sul proprio PC; è consigliato pertanto salvarli periodicamente sul Server, al fine di evitarne la perdita (es. nel caso in cui si guasti l'Hard Disk).
2. Il Centro Elaborazione esegue sistematicamente il salvataggio dei dati contenuti sui server e procede al salvataggio su supporti magnetici.

3. E’ vietato salvare posta elettronica, profili utente sulle cartelle di rete.

Art. 12 Aggiornamenti

1. Gli aggiornamenti del sistema operativo sono necessari, oltre che essere un obbligo di legge, al fine di proteggere il PC e l’intera rete. Questi aggiornamenti vengono effettuati automaticamente di norma alle ore 13, una volta approvati dall'amministratore di sistema.
2. E’ tassativamente vietato all’utente ogni sorta di aggiornamento del software installato.

Art. 13 Installazione degli applicativi sui personal computer o su Server

1. Ogni intervento che richieda l’installazione o l’aggiornamento di software su personal computer o Server e comunque su apparati dell’Ente deve essere concordato con l’Amministratore del Sistema.
2. Tutte le installazioni dovranno essere assistite dal personale tecnico dell’Ente.
3. E’ dato obbligo ai singoli Settori di trasmettere al Servizio CED i CD di installazione e l’eventuale documentazione forniti dalle Società o Enti esterni.

Art. 14 Gestione degli accessi alla rete e dei permessi

1. Tutte le richieste per eventuali abilitazioni, creazioni di utente, modifiche, ecc., dovranno essere inviate mediante gli appositi moduli scaricabili dalla rete intranet.

Art. 15 Richieste di assistenza tecnica (Help Desk)

1. L’attivazione di una chiamata per le richieste di assistenza tecnica hardware e/o software deve avvenire mediante intranet.
2. Tutte le richieste di acquisto di materiale di consumo delle stampanti, come toner, cartucce, ecc., devono essere inoltrate all’Ufficio Economato.

Art. 16 Osservanza delle disposizioni in materia di Privacy

1. E’ obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, così come altresì indicato nella lettera di incarico per il trattamento dei dati di cui al D. Lgs. n. 196 del 30 giugno 2003.
2. Il mancato rispetto o la violazione delle regole contenute nel D.Lgs. n. 196 del 30 giugno 2003 è perseguibile con le azioni civili e penali previste.
3. Il mancato rispetto delle norme contenute nel presente regolamento può comportare l’applicazione di sanzioni disciplinari, in ottemperanza alle disposizioni disciplinari di cui ai CCNL.
4. Il presente regolamento, unitamente all’allegato sul controllo a distanza dei lavoratori relativamente all’utilizzo di internet e della posta elettronica, costituisce un’appendice al codice disciplinare dell’Ente, ai sensi dell’art. 54 – comma 5 – del D. Lgs. n. 165/2001 ed è soggetto ad affissione all’Albo Pretorio dell’Ente e in luogo accessibile a tutti i dipendenti, e a pubblicazione nella rete intranet provinciale.

Provincia di Lecco

Appendice al

“Regolamento per il corretto utilizzo degli strumenti informatici e telematici”

sul controllo a distanza dei lavoratori

relativamente all’utilizzo di internet

e posta elettronica

Articolo 1 – Oggetto
La presente disciplina regola le modalità con le quali la Provincia di Lecco potrà accertare e quindi reprimere le condotte illecite dei dipendenti utilizzatori di internet e della posta elettronica, ai sensi dell'art. 4 della legge 300/70 (Statuto dei Lavoratori).

Articolo 2 – Controllo sull'utilizzo di Internet: siti web interdetti
La Provincia di Lecco potrà stabilire ed aggiornare un elenco di siti internet verso i quali sia *a priori* interdetta la navigazione (black list). Con cadenza periodica tale elenco, se adottato, dovrà essere inviato in informazione successiva alle parti sindacali al fine dell'accertamento dell'insussistenza di violazioni di diritti costituzionalmente garantiti (libertà di opinione, libertà di associazione, libertà sindacale). Eventuali deroghe all'accessibilità dei siti interdetti dovranno essere autorizzate dal Dirigente del Settore Organizzazione e Gestione Risorse Umane, su richiesta del Dirigente del Settore interessato, qualora tale accessibilità sia funzionale alle esigenze di servizio.

Articolo 3 – Modalità e limiti dei controlli sull'utilizzo di internet
Ai soli fini di accertare e quindi reprimere condotte illecite dei lavoratori utilizzatori di internet l'Ente può, a sua tutela, effettuare verifiche a campione od anche in via sistematica sugli accessi effettuati mediante idonei programmi diagnostici informatici. E' comunque esclusa la possibilità di effettuare controlli sugli accessi internet mediante impianti audiovisivi.
I controlli dovranno essere in prima battuta svolti in modo tale da ridurre al minimo la riconducibilità ai dipendenti, salva, ovviamente, la possibilità in caso di abuso di decriptare il nominativo dell'utilizzatore.

Art. 4 – Repressione dell'abuso di internet
Qualora, ad esito del controllo, l'Ente rilevi delle anomalie sull'utilizzo di internet che possano essere configurate quali abusi, si procederà a comunicare l'avvio del procedimento disciplinare all'interessato e, per conoscenza, al relativo Dirigente del Settore. A seguito dell'accertamento della condotta illecita e, quindi, dell'adozione del provvedimento disciplinare l'Ente procederà altresì a segnalare all'Autorità competente o a reprimere l'abuso secondo la normativa vigente.
Ai fini della corretta interpretazione della presente disciplina, per abuso di utilizzo di internet, oltre all'uso in difformità di quanto disciplinato dal "Regolamento per il corretto utilizzo degli strumenti informatici e telematici", si intende quanto segue:
- visita di siti web per motivi non pertinenti al proprio servizio o alla propria funzione, attuata con modalità e tempi tali da incidere negativamente sull'ordinaria attività;
- visita di siti web interdetti;
- scaricare e installare software senza una preventiva autorizzazione del Responsabile del Servizio CED;
- utilizzo mediante internet di funzionalità informatiche già rese disponibili dall'Ente;
- manomissioni dei sistemi di protezione e/o delle configurazioni dei personal computer;
- azioni aventi rilevanza penale, con riferimento a qualunque condotta penalmente rilevante anche se non contemplata fra i reati contro la Pubblica Amministrazione;
- azioni commesse con dolo o colpa grave che mettano a repentaglio la sicurezza e l'integrità del sistema informatico provinciale e dei dati personali trattati;
- azioni in frode alle misure di sicurezza comunque inerenti i punti precedenti.

Art. 5 – Utilizzo di posta elettronica - Tutela preventiva
La Provincia di Lecco dà attuazione a quanto previsto dalla Deliberazione n. 13/2007 del Garante per la protezione dei dati personali e, pertanto:
- il datore di lavoro rende disponibili, laddove possibile, indirizzi di posta elettronica istituzionali condivisi tra più lavoratori, eventualmente affiancandoli a quelli individuali;

- il datore di lavoro mette a disposizione e prescrive a ciascun lavoratore di avvalersi di apposite funzionalità di sistema, di agevole utilizzo, che consentono di inviare automaticamente, in caso di assenze (ad es., per ferie o attività di lavoro fuori sede), messaggi di risposta contenenti le "coordinate" (anche elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto della struttura. In caso di eventuali assenze non programmate (ad es., per malattia), qualora il lavoratore non possa attivare la procedura descritta, l'Ente, perdurando l'assenza oltre i tempi necessari all'espletamento della propria attività connessa alle informazioni contenute nella casella di posta elettronica in tempo utile per il rispetto dei termini procedimentali, può disporre, mediante il Responsabile della Sicurezza Informatica o suo delegato, l'attivazione di un analogo accorgimento, avvertendo gli interessati;
- in previsione della possibilità che, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica, l'interessato deve essere messo in grado di delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Il fiduciario deve essere designato dal dipendente e nominato dal Dirigente del Settore interessato.
- i messaggi di posta elettronica dovranno contenere un avvertimento ai destinatari nel quale sia dichiarata l'eventuale natura non personale dei messaggi stessi, precisando se le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente e con eventuale rinvio al presente accordo.

Art. 6 – Controllo a distanza sull'utilizzo della posta elettronica

Così come altresì precisato dall'art. 6 del vigente "Regolamento per il corretto utilizzo degli strumenti informatici e telematici", le caselle di posta elettronica istituzionale sono strumenti di lavoro.

Ai soli fini di accertare e quindi reprimere condotte illecite dei lavoratori utilizzatori della posta elettronica l'Ente può, a sua tutela, effettuare verifiche a campione od anche in via sistematica mediante idonei programmi diagnostici informatici. E' comunque esclusa la possibilità di effettuare controlli sull'utilizzo della posta elettronica mediante impianti audiovisivi.

Le presenti disposizioni inerenti il controllo a distanza dell'utilizzo di internet sono estese, in quanto applicabili, al controllo previsto dal presente articolo sull'utilizzo della posta elettronica, con le precisazioni di seguito riportate.

In via generale il controllo difensivo dell'Ente potrà essere eventualmente esercitato in relazione ai destinatari delle e-mail in uscita.

Relativamente alle e-mail in entrata, il controllo difensivo dell'Ente potrà essere esercitato sui mittenti solamente per verificare l'eventuale avvenuta iscrizione degli utilizzatori della posta elettronica *a mailing list* per motivi non istituzionali o non pertinenti al servizio o alle funzioni svolte, con conseguente abuso dell'utilizzo di internet che non sia stato precedentemente rilevato.

Per abuso di utilizzo della poste elettronica si intende quanto segue:

- nel caso di iscrizione a *mailing list,* visita di siti web per motivi non pertinenti al proprio servizio o alla propria funzione, attuata con modalità e tempi tali da incidere negativamente sull'ordinaria attività di servizio, qualora ciò non abbia rilevanza penale;
- nel caso di iscrizione a mailing list, visita a siti web interdetti;
- farsi inviare software;
- diffusione di software di proprietà dell'ente o di terzi,
- diffusione di banche dati di cui l'Ente sia titolare;
- utilizzo di funzionalità informatiche già rese disponibili dall'Ente;
- utilizzo della posta elettronica per scopi puramente privati;

- azioni aventi rilevanza penale, con riferimento a qualunque condotta penalmente rilevante anche se non contemplata fra i reati contro la Pubblica Amministrazione;
- azioni in frode alle misure di sicurezza inerenti i punti precedenti.

E' esclusa qualsiasi forma di controllo sull'utilizzo della posta elettronica diversa da quelle previste nel presente articolo.

Art. 7 – Pubblicità - Entrata in vigore

Il Dirigente del Settore Organizzazione e Gestione Risorse Umane è incaricato di rendere noto il contenuto della presente disciplina ai dipendenti della Provincia di Lecco mediante affissione del medesimo all'Albo Pretorio dell'Ente e in luogo accessibile a tutti i dipendenti, e mediante pubblicazione nella rete intranet provinciale.

La presente disciplina entrerà in vigore all'atto del suo recepimento da parte dell'organo di governo.