Prot. n. 2104/A.20 Carapelle, 03.06.2014

REGOLAMENTO SULL' UTILIZZO DI STRUMENTI INFORMATICI, TELEMATICI, INTERNET E MAIL.

INTRODUZIONE E RIFERIMENTI NORMATIVI

Le realtà aziendali sono andate caratterizzandosi in questi ultimi anni per l'elevato uso delle tecnologie informatiche e telefoniche che, se da un lato hanno consentito l'introduzione di innovative tecniche di gestione dell'impresa, dall'altro hanno anche dato origine a numerose problematiche relative all'utilizzo degli strumenti informatici/telefonici forniti dall'azienda ai propri collaboratori per lo svolgimento delle mansioni e compiti affidati.

In questo senso, viene fortemente sentita dai datori di lavoro la necessità di porre in essere adeguati sistemi di controllo sull'utilizzo di tali strumenti da parte dei dipendenti/collaboratori e di sanzionare conseguentemente quegli usi scorretti che, oltre ad esporre l'azienda stessa a rischi tanto patrimoniali quanto penali, possono di per sé considerarsi contrari ai doveri di diligenza e fedeltà previsti dagli artt. 2104 e 2105 del Codice civile.

I controlli sull'uso degli strumenti informatici/telefonici tuttavia, devono garantire tanto il diritto del datore di lavoro di proteggere la propria organizzazione, essendo i computer ed i telefoni aziendali strumenti di lavoro la cui utilizzazione personale è preclusa, quanto il diritto del lavoratore a non vedere invasa la propria sfera personale, e quindi il diritto alla riservatezza ed alla dignità come sanciti dallo Statuto dei lavoratori e dal Codice sulla privacy.

I regolamenti aziendali (quali quello proposto) ed in genere le "policy" aziendali che dettano le regole sull'uso degli strumenti informatici e telematici, non sono comunque sostitutive della procedura prevista dal 2° comma dell'art. 4 dello Statuto dei lavoratori in materia di controlli leciti, nei casi in cui questa procedura sia necessaria.

Tuttavia, proprio l'adozione di un regolamento aziendale che evidenzi la natura non personale della casella di posta assegnata e ne definisca le modalità d'uso ed i possibili controlli, rappresenta un utile strumento per evitare la configurabilità di un reato.

Alla luce delle considerazioni sopra espresse e tenuto opportunamente conto delle Linee guida recentemente emanate dall'Autorità garante per la protezione dei dati personali, con propria deliberazione n. 13 del 1 marzo 2007, sulla disciplina della navigazione in internet e sulla gestione della posta elettronica nei luoghi di lavoro, il Coordinamento legale delle associazioni industriali del triveneto, congiuntamente al Coordinamento dei servizi sindacali e con la collaborazione degli esperti delle Associazioni in materia di Information Technology, ha elaborato uno schema di regolamento utilizzabile dalle imprese proprio per disciplinare le condizioni per il corretto utilizzo degli strumenti informatici/telefonici da parte dei dipendenti e/o collaboratori.

Il regolamento di seguito proposto, elaborato sull'impronta del suddetto schema, essendo rilevante ai fini delle eventuali azioni disciplinari attivabili dal datore di lavoro nei confronti del dipendente, è stato redatto anche tenendo opportunamente conto, da una parte delle disposizioni contenute nella Legge. n. 300/1970 in tema di provvedimenti disciplinari (art. 7), dall'altra delle indicazioni emerse nelle prime sentenze di merito e di legittimità pronunciatesi sull'argomento.

Vengono inoltre considerati gli specifici obblighi previsti dal Codice della privacy (D.Lgs. n. 196/2003 e successive modifiche ed integrazioni) e dall'art. 29, 1°comma del D.Lgs. n. 242/1996 (in tema di controlli operati mediante il sistema informatico aziendale), nonché gli obblighi previsti dal disciplinare tecnico sulle misure minime di sicurezza allegato allo stesso Codice.

Il regolamento ha lo scopo di informare gli interessati sulle finalità del controllo e sulle specifiche tecnologie adottate per effettuarlo. Particolare attenzione dovrà comunque venir prestata all'attività di controllo della navigazione internet qualora, mediante l'individuazione dei contenuti dei siti visitati, si determini un trattamento di dati sensibili per i quali deve sempre essere rispettato il principio dell'indispensabilità (art. 26, 4°comma lett. c) del Codice).Il regolamento, inoltre, oltre a dettare una disciplina per l'utilizzo degli strumenti informatici/telefonici aziendali, vuole costituire un utile strumento per sensibilizzare il personale su altri aspetti altrettanto importanti nella gestione dei sistemi informatici aziendali, quali il rispetto della normativa sulla tutela legale del software (e quindi il controllo sulla regolarità del software presente nello stesso sistema informatico), e quella sulla tutela del know-how aziendale, quando queste importanti informazioni di proprietà dell'impresa sono custodite nel sistema informatico.

Tra l'altro, se correttamente applicato e fatto rispettare, il regolamento può risultare anche un efficace strumento per limitare il rischio di insorgenza della responsabilità amministrativa a carico della società o del dipendente.

(Il presente regolamento è stato redatto tenendo conto delle linee guida del Garante della Privacy emanate con delibera n. 13 del 1° marzo 2007.

INDICE

PREMESSA

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete Internet dai Personal Computer, espone questa Istituzione scolastica e gli utenti (dipendenti e collaboratori della stessa) a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (legge sul diritto d'autore e legge sulla privacy, fra tutte), creando evidenti problemi alla sicurezza ed all'immagine dell'Azienda stessa.

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro, l'Istituto Comprensivo Statale " Carapelle" ha adottato un Regolamento interno, di seguito declinato, diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati.

Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni già fornite a tutti gli incaricati in attuazione del D.Lgs. 30 giugno 2003 n. 196 e del Disciplinare tecnico (Allegato B al citato decreto legislativo) contenente le misure minime di sicurezza, nonché

integrano le informazioni già fornite agli interessati anche verbalmente in ordine alle ragioni e alle modalità dei possibili controlli o alle conseguenze di tipo disciplinare in caso di violazione delle stesse.

Considerato inoltre che questa amministrazione, nell'ottica di uno svolgimento proficuo e più agevole della propria attività, ha da tempo deciso di mettere a disposizione dei propri collaboratori che ne necessitassero per il tipo di funzioni svolte, telefoni e mezzi di comunicazione efficienti (computer a postazione fissa, portatili, etc.), sono state inserite nel regolamento alcune clausole relative alle modalità ed i doveri che ciascun dipendente deve osservare nell'utilizzo di tale strumentazione.

1. Entrata in vigore del regolamento e pubblicità

1.1 Il nuovo regolamento entrerà in vigore il 03.06.2014. Con l'entrata in vigore del presente regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.

1.2 Copia del regolamento, oltre ad essere affisso nella bacheca aziendale verrà pubblicata sul sito della scuola: www.scuolacarapelle.it

2. Campo di applicazione del regolamento

2.1 Il nuovo regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori dell'istituzione a prescindere dal rapporto contrattuale con la stessa intrattenuto (lavoratori somministrati, collaboratore a progetto, in stage, ecc.).

2.2 Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni dipendente e collaboratore (collaboratore a progetto, in stage, agente, ecc.) in possesso di specifiche credenziali di autenticazione. Tale figura potrà anche venir indicata quale "incaricato del trattamento".

3. Utilizzo del Personal Computer

3.1 **Il Personal Computer affidato all'utente è uno strumento di lavoro**. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Il personal computer deve essere custodito con cura evitando ogni possibile forma di danneggiamento.

3.2 Il personal computer dato in affidamento all'utente permette l'accesso alla rete informatica della scuola solo attraverso specifiche **credenziali di autenticazione** come meglio descritto al successivo punto 4 del presente Regolamento.

3.3 Il Dirigente Scolastico rende noto che solo il personale incaricato, nelle persone degli Ing. Luigi Martino (in qualità anche di amministratore di sistema) e Mario Zagaria, è stato autorizzato a compiere interventi nel sistema informatico della scuola diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi,

manutenzione hardware etc.). Detti interventi, in considerazione dei divieti di cui ai successivi punti nn. 8.2 e 9.1, potranno anche comportare l'accesso in qualunque momento, ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, nonché alla verifica sui siti internet acceduti dagli utenti abilitati alla navigazione esterna. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'Azienda, si applica anche in caso di assenza prolungata o di impedimento anche dell'utente.

3.4 Il personale incaricato del servizio di assistenza tecnica ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento viene effettuato su chiamata dell'utente o, in caso di oggettiva necessità**,** a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.

3.5 Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal personale del servizio di assistenza tecnica per conto dell'Istituto Comprensivo Carapelle né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre Virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione espone la stessa amministrazione a gravi responsabilità civili; si evidenzia inoltre che le violazioni della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate anche penalmente.

3.6 Salvo preventiva espressa autorizzazione del personale del servizio di assistenza tecnica, non è consentito all'utente modificare le caratteristiche impostate sul proprio PC né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, …).

3.7 Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale del servizio nel caso in cui siano rilevati virus ed adottando quanto previsto dal successivo punto 10 del presente Regolamento relativo alle procedure di protezione antivirus

3.8 Il Personal Computer deve essere spento ogni giorno prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo. 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 provarne in seguito l'indebito uso**.**

4. Gestione ed assegnazione delle credenziali di autenticazione

4.1 Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dall'amministratore di sistema.

4.2 Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), associato ad una parola chiave (password) riservata che dovrà venir custodita dall'incaricato con la massima diligenza e non divulgata. Non è consentita l'attivazione della

password di accensione (bios), senza preventiva autorizzazione da parte dell'amministratore di sistema.

4.3 La parola chiave, formata da lettere (maiuscole o minuscole) e/o numeri, anche in combinazione fra loro, deve essere composta da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato.

4.4 È necessario procedere alla modifica della parola chiave a cura dell'utente, incaricato del trattamento, al primo utilizzo e, successivamente, almeno ogni sei mesi.

4.5 Qualora la parola chiave dovesse venir sostituita, per decorso del termine sopra previsto e/o in quanto abbia perduto la propria riservatezza, si procederà in tal senso d'intesa con l'amministratore di sistema.

4.6 Soggetto preposto alla custodia delle credenziali di autenticazione è il Dirigente scolastico oltre all'amministratore di sistema.

5. Utilizzo della rete informatica dell'amministrazione scolastica

5.1 Per l'accesso alla rete informatica della scuola ciascun utente deve essere in possesso della specifica credenziale di autenticazione.

5.2 È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato. Le parola chiave d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.

5.3 Le cartelle utenti presenti nei server della scuola sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità vengono svolte regolari attività di controllo, amministrazione e back up da parte del personale del Servizio ICT. (Eventuale: Si ricorda che tutti i dischi o altre unità di memorizzazione locali (es. disco C: interno PC) non sono soggette a salvataggio da parte del personale incaricato del Servizio ICT. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo utente).

Il personale del servizio di assistenza tecnica può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.

5.4 Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

6. Utilizzo e conservazione dei supporti rimovibili

6.1 Tutti i supporti magnetici rimovibili (dischetti, CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati sensibili nonché informazioni costituenti know-how aziendale, devono essere

trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.

6.2 Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, ciascun utente dovrà contattare il personale del Servizio ICT e seguire le istruzioni da questo impartite.

6.3 In ogni caso, i supporti magnetici contenenti dati sensibili devono essere dagli utenti adeguatamente custoditi in armadi chiusi.

6.4 E' vietato l'utilizzo di supporti rimovibili personali.

6.5 L'utente è responsabile della custodia dei supporti e dei dati aziendali in essi contenuti.

7. Utilizzo di PC portatili

7.1 L'utente è responsabile del P assegnatogli e deve custodirlo con diligenza durante l'utilizzo nel luogo di lavoro.

7.2 Ai PC portatili si applicano le regole di utilizzo previste dal presente regolamento, con particolare attenzione alla rimozione di eventuali file elaborati prima della riconsegna.

7.3 I PC portatili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.

7.4 Tali disposizioni si applicano anche nei confronti di incaricati esterni quali esperti ecc.

8. Uso della posta elettronica

8.1 **La casella di posta elettronica assegnata all'utente è uno strumento di lavoro.** Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

8.2 È fatto divieto di utilizzare le caselle di posta elettronica per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per:

- l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es.mp3) non legati all'attività lavorativa;
- l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list;
- la partecipazione a catene telematiche. Se si dovessero peraltro ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al personale dell'assistenza. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.

8.3 La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

8.4 Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per l'istituzione scolastica ovvero contenga documenti da

considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analoga dicitura, deve essere visionata dal Dirigente scolastico o dal DSGA se autorizzato.

8.5 È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario. Si evidenzia però che le comunicazioni ufficiali, da inviarsi mediante gli strumenti tradizionali (fax, posta, …), devono essere autorizzate e firmate dalla Direzione, a seconda del loro contenuto e dei destinatari delle stesse.

8.6 È obbligatorio porre la massima attenzione nell'aprire i file attachements di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

9. Navigazione in Internet

9.1. **Il PC assegnato al singolo utente ed abilitato alla navigazione in Internet costituisce uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa**. È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa.

9.2 In questo senso, a titolo puramente esemplificativo, **l'utente non potrà utilizzare internet** per:

- l'upload o il download di software gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa (filmati e musica) e previa verifica dell'attendibilità dei siti in questione (nel caso di dubbio, dovrà venir a tal fine contattato il personale del Servizio di assistenza;

- l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dalla Direzione e comunque nel rispetto delle normali procedure di acquisto;

- ogni forma di registrazione a siti i cui contenuti non siano strettamente legate all'attività lavorativa;

- la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

- l'accesso, tramite internet, a caselle webmail di posta elettronica personale.

9.3 Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, l'Istituzione scolastica rende peraltro nota la possibile adozione di uno specifico sistema di blocco o filtro automatico che prevengano determinate operazioni quali l'upload o l'accesso a determinati siti inseriti in una black list.

9.4 Gli eventuali controlli, compiuti dal personale incaricato del Servizio di assistenza ai sensi del precedente punto 3.3, potranno avvenire mediante un sistema di controllo dei contenuti.

10. Protezione antivirus

10.1 Il sistema informatico dell'Istituto Comprensivo è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo.

10.2 Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer nonché segnalare prontamente l'accaduto al personale del Servizio.

10.3 Ogni dispositivo magnetico di provenienza esterna all'Azienda dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al personale del Servizio ICT.

11. Utilizzo dei telefoni, fax e fotocopiatrici aziendali

11.1 **Il telefono aziendale affidato all'utente è uno strumento di lavoro.** Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti l'attività lavorativa stessa. La ricezione o l'effettuazione di telefonate personali è consentito solo nel caso di comprovata necessità ed urgenza, mediante il telefono fisso aziendale a disposizione

11.2 È vietato l'utilizzo dei fax aziendali per fini personali, tanto per spedire quanto per ricevere documentazione, salva diversa esplicita autorizzazione.

11.3 È vietato l'utilizzo delle fotocopiatrici aziendali per fini personali.

12. Osservanza delle disposizioni in materia di Privacy

12.1 È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, come indicato nella lettera di designazione ad incaricato del trattamento dei dati ai sensi del Disciplinare tecnico allegato al D.Lgs. n. 196/2003.

13. Accesso ai dati trattati dall'utente

13.1 Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.) o per finalità di controllo e programmazione dei costi aziendali (ad esempio, verifica costi di connessione ad internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà della Direzione, anche tramite il personale del Servizio di assistenza o l'amministratore di sistema, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici aziendali e ai documenti ivi contenuti.

14. Sistemi di controlli graduali

14.1 In caso di anomalie, il personale incaricato del servizio ICT effettuerà controlli anonimi che si concluderanno con un avvisi generalizzati diretti ai dipendenti dell'area o del settore in cui è stata rilevata l'anomalia, nei quali si evidenzierà l'utilizzo irregolare degli strumenti aziendali e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. Controlli su base individuale potranno essere computi solo in caso di successive ulteriori anomalie.

15. Sanzioni

15.1 È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente regolamento. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dal vigente CCNL nonché con tutte le azioni civili e penali consentite.

16. Aggiornamento e revisione

16.1 Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate al presente Regolamento. Le proposte verranno esaminate dalla Direzione e dall'amministratore di sistema.

16.2 Il presente Regolamento potrebbe essere soggetto a revisione annuale.

f.to IL DIRIGENTE SCOLASTICO
Dott.ssa Antonella lo SURDO