**Centro Provinciale per l'Istruzione degli Adulti di Caserta**
**Unità Amministrativa: Vicolo G.F. Ghedini, 2, 81100, Caserta (CE)**
**Recapito Telefonico:0823341601; E-mail: cemm18000t@istruzione.it**
**PEC: cemm18000t@pec.istruzione.it - Sito web: www.cpiacaserta.gov.it**
**Codice Meccanografico: cemm18000t -Codice Fiscale: 93093640618- Codice Univoco: UFHO5J**

# REGOLAMENTO
## PER LA SICUREZZA INFORMATICA E L'UTILIZZO DELLE POSTAZIONI

Premessa

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet dai Personal Computer, espone **Centro Provinciale per l'Istruzione degli Adulti di Caserta** ai rischi di un coinvolgimento sia patrimoniale che penale, creando problemi alla sicurezza e all'immagine dello stesso.

L'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente sono basilari in un qualsiasi ambiente di lavoro.

L'Istituto ha adottato il presente regolamento per contribuire alla massima diffusione della cultura della sicurezza ed evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati.

Il Regolamento di seguito riportato viene incontro quindi alla necessità di disciplinare le condizioni per il corretto utilizzo degli strumenti informatici da parte di tutto il personale scolastico e degli alunni e contiene informazioni utili per comprendere cosa può fare ogni soggetto per contribuire a garantire la sicurezza informatica di tutta l'istituzione scolastica.

### 1. Utilizzo del Personal Computer

1.2 I Personal Computer affidati al personale di segreteria, ai docenti e agli allievi sono strumenti di lavoro. Ognuno è responsabile dell'utilizzo delle dotazioni informatiche ricevute in assegnazione. Ogni utilizzo non inerente all'attività lavorativa e/o didattica può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

1.3 Non è consentita l'attivazione della password d'accensione (bios), senza preventiva autorizzazione da parte del D.S. o del D.S.G.A.

1.4 Non è consentito all'utente modificare le caratteristiche hardware e software impostate sul proprio PC, salvo previa autorizzazione esplicita da parte del D.S.

1.5 Il Personal Computer deve essere spento prima di lasciare gli uffici o i laboratori o in caso di assenze prolungate dall'ufficio o dal laboratorio.

1.6 Le informazioni archiviate informaticamente devono essere esclusivamente quelle previste dalla legge o necessarie all'attività lavorativa e/o didattica.

1.7 Negli uffici di segreteria particolare attenzione deve essere prestata alla duplicazione dei dati.

E' infatti assolutamente da evitare un'archiviazione ridondante.

1.8 La tutela della gestione locale di dati sui PC è demandata all'utente finale che dovrà effettuare, con frequenza opportuna, i salvataggi su supporti magnetici e/o di rete e la conservazione degli stessi in luogo idoneo.

1.9 Non è consentita l'installazione di programmi diversi da quelli autorizzati dal D.S.

1.10 Su richiesta di un docente e per gli usi didattici è possibile installare software aggiuntivo che in ogni caso deve essere coperto da licenza d'uso.

1.11 Non è consentita la riproduzione o la duplicazione di programmi informatici ai sensi delle Legge n.128 del 21.05.2004.

## 2 Utilizzo della rete LAN

2.1 L'accesso alla rete interna è protetto da password; per l'accesso deve essere utilizzato il proprio profilo personale (username e password).

2.2 E' fatto divieto di utilizzare la rete interna per fini non espressamente autorizzati.

2.3 E' vietato connettere in rete stazioni di lavoro se non dietro esplicita e formale autorizzazione del D.S.

2.4 E' vietato condividere cartelle in rete sia dotate di password, sia sprovviste di password se non dietro esplicita e formale autorizzazione del D.S.

2.5 E' vietato monitorare ciò che transita in rete.

2.6 E' vietata l'installazione non autorizzata di modem che sfruttino il sistema di comunicazione telefonico per l'accesso a banche dati esterne o interne all'Istituto

## 3 Gestione delle Password

3.1 Le password d'ingresso alla rete, di accesso ai vari programmi in rete per i trattamenti dei dati e ad Internet, sono attribuite dal D.S.G.A.

3.2 L'utente è tenuto a conservare nella massima segretezza la parola di accesso alla rete ed ai sistemi e qualsiasi altra informazione legata al processo di autenticazione.

3.3 L'utente è tenuto a scollegarsi dal sistema ogni qualvolta sia costretto ad assentarsi dal locale

nel quale è ubicata la stazione di lavoro o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima: 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.

3.4 La password deve essere immediatamente sostituita, dandone comunicazione al D.S.G.A nel caso si sospetti che la stessa abbia perso la segretezza.

## 4 Uso della posta elettronica

4.1 Le caselle di posta dell'Istituto e quella eventualmente assegnata dall'Istituto all'utente, sono strumenti di lavoro.

4.2 Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse (art. 615 comma 5 e segg. c.p.).

4.3 Nel caso di mittenti sconosciuti o messaggi insoliti, per non correre il rischio di essere infettati da virus occorrerà cancellare i messaggi senza aprirli.

4.4 Nel caso di messaggi provenienti da mittenti conosciuti ma che contengono allegati sospetti (file con estensione .exe .scr .pif .bat .cmd), questi ultimi non devono essere aperti.

4.5 Evitare che la diffusione incontrollata di "Catene di Sant'Antonio" (messaggi a diffusione capillare e moltiplicata) limiti l'efficienza del sistema di posta.

4.6 Nel caso in cui si debba inviare un documento all'esterno della scuola, è preferibile utilizzare un formato protetto da scrittura (ad esempio il formato Acrobat *.pdf).

4.7 Utilizzare, nel caso di invio di allegati pesanti, i formati compressi (*.zip *.rar *.jpg)

4.8 L'iscrizione a "mailing list" esterne è concessa solo per motivi professionali, prima di iscriversi occorre verificare in anticipo se il sito è affidabile.

4.9 Le caselle di posta devono essere mantenute in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

4.10 E' obbligatorio controllare 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).

4.11 L'abilitazione alla posta esterna ad uso privato deve essere preceduta da regolare richiesta al D.S.

4.12 Il contenuto dei messaggi privati di posta elettronica riguardano forme di corrispondenza assistite da garanzie di segretezza tutelate dalla Costituzione, dal Codice Penale e dal Codice dell'amministrazione digitale.

## 5 Uso della rete Internet e dei relativi servizi

5.1 L'abilitazione ad Internet deve essere preceduta da regolare richiesta al D.S.

5.2 E' assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati alle attività didattiche e/o lavorative.

5.3 Si fa esplicito divieto di servirsi della rete Internet per qualsiasi altra utilizzazione, con particolare riferimento al trattamento di dati personali dell'utente o di terzi.

5.4 Non possono essere utilizzati modem privati per il collegamento alla rete.

5.5 E' vietato l'uso non autorizzato di account, codici di accesso o numeri di identificazione IP.

5.6 E' fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dal D.S.

5.7 I minori possono accedere ad Internet solo sotto il controllo diretto di un docente.

5.8 E' vietata la partecipazione a Forum non professionali, l'utilizzo di Instant messaging e chat, di bacheche elettroniche, di telefonate virtuali e le registrazioni in guest books anche utilizzando pseudonimi o nicknames (esclusi gli strumenti autorizzati).

5.9 L'Istituto non garantisce agli utenti la riservatezza dei percorsi da loro compiuti durante la navigazione, che possono essere assoggettati a controllo a fini di rilevazione statistica o ad altri fini previsti dalla legge.

A norma delle vigenti leggi, l'utente è responsabile civilmente e penalmente per l'uso fatto dell'accesso ad Internet. L'Istituto si riserva di denunciare alle autorità competenti l'utente che si renda direttamente responsabile di attività illecite compiute durante la fruizione del servizio.

L'Istituto predisporrà particolari restrizioni sulla sua rete: provvederà al filtraggio del traffico mediante apparati di rete "firewall". Dovranno essere filtrati almeno tutti quei collegamenti vietati dalla vigente normativa, dalla User Policy del GARR e dalle regole internazionali dell'RFC 1855 "Netiquette Guidelines", nonché quelli verso server, apparati e personal computer non offerenti servizi ufficiali e/o a valenza esterna. L'Istituto garantirà comunque l'accesso a tutte le basi dati presenti in Internet utili alla didattica e ai servizi amministrativi.

Il presente regolamento può essere suscettibile di modifiche con le stesse modalità previste per la sua approvazione.

Caserta 02/10/2018