Regolamento informatico interno ai fini privacy

REGOLAMENTO INFORMATICO INTERNO VALIDO AI SENSI DEL D.LG. 196/03 PER FINI FORMATIVI IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

UTILIZZO STRUMENTAZIONE HARDWARE E SOFTWARE

1. È fatto divieto installare sulla strumentazione in uso, hardware fisso o removibile (ad esempio chiavette, internet, cellulari, ecc.) se non per attività didattica.
2. Il CFP Vantini si riserva di eliminare qualsiasi elemento hardware fisso o removibile la cui installazione non sia stata appositamente prevista o autorizzata o non sia strettamente attinente all'attività didattica.
3. E' obbligatorio attivate su ogni hardware uno screen saver protetto da password in modo che in caso di allontanamento dalla propria postazione..
4. Sui PC dotati di scheda audio, non è consentito l'ascolto di programmi, files audio o video in streeming, se non a fini prettamente didattici.
5. Qualora si rendessero necessarie modifiche alle configurazioni impostate sul PC in uso o istallazioni di nuovi programmi, occorre effettuarne richiesta tramite la direzione che informerà l'amministratore di sistema.
6. In caso di furto o smarrimento di dispositivi portatili e/o tablet, effettuare una comunicazione alla direzione.
7. I software autorizzati e installati sui dispositivi in uso sono:

Microsoft OFFICE VERSIONI DA OFFICE XP A 2016
ADOBE ACROBAT READER VERSIONI DA 8 A DC
GESTIONE POSTA ELETTRONICA TUNDERBIRD
AUTOCAD MECHANICAL VERS. 2009 COMPLETO AULA CAD
SOLID WORKS AULA CNC
ANTIVIRUS PANDA CLOUD PROTECTIN PC AMMINISTRATIVI E PROFESSORI
ANTIVIRUS PANDA CLOUD PROTECTIN PLUS PC AULE STUDENTI
ZELIO SOFTWARE AULA CNC
PROFICAD AULA CAD/CNC
SOFTWARE HEIDENAIN AULA CNC
SOFTWARE SELCA AULA CNC
WIN NC – AULA CNC
DATA PILOT AULA CNC
DEEP FREEZE AULA CNC-CAD
SOFWARE TITEX
SOFTWARE GIBS CAM
OPEN OFFICE PC SEGRETERIA

ACCESSO ED USO DEI SISTEMI

1. Ogni utente la cui mansione prevede l'accesso a dati personali contenuti nelle cartelle di rete, si connette alla rete tramite autenticazione univoca personale.
2. Le credenziali ad autenticazione univoca e personale devono essere richieste alla direzione che provvederà a fornire la prima credenziale di accesso da modificare al primo accesso da parte dell'utente .
3. Le credenziali di autenticazione alla rete devono essere custodite e preservate dalla conoscibilità di soggetti interni e/o esterni all'ente.
4. In nessun caso devono essere annotate password personali in chiaro sia su supporto cartaceo che informatico.
5. I requisiti minimi di complessità delle password sulla base della vigente normativa privacy sono:
    a. redazione con caratteri maiuscoli e/o minuscoli;
    b. composizione con inclusione di simboli, numeri, punteggiatura e lettere;
    c. caratteri non inferiori a 8 (ad eccezione dei sistemi operativi che non supportano tali requisiti);
    d. password non agevolmente riconducibile all'identità del soggetto che la gestisce. Pertanto, la password non deve essere basata su informazioni personali, riferimenti familiari o comunque dati inerenti direttamente il soggetto titolare della password stessa.
6. Qualora l'intestatario della password ritenga che un soggetto non autorizzato possa essere venuto a conoscenza della propria password, dovrà provvedere immediatamente a comunicare l'episodio al custode password.
7. Non debbono essere utilizzate per l'accesso ai portali le opzioni di "compilazione automatica" o remember password, presenti nei browser o in altre applicazioni.
8. L'utente ha l'obbligo di non alterare la funzione "cambio password" dell'accesso alla rete che obbliga a modificare la password con cadenza trimestrale/semestrale.
9. La scadenza password dei portali utilizzati per scopi lavorativi sono regolate dal gestore del portale stesso.
10. In caso di dispositivi mobili e/o tablet è necessario impostare un codice accesso e/o password per evitare che nessun altro utente possa consultare i dati in esso contenuti in caso di abbandono, furto o smarrimento.

INSTALLAZIONE PROGRAMMI

1. Sul pc in uso non deve essere installato nessun software. Qualsiasi richiesta di installazione deve essere effettuata mediante direzione
2. Si ricorda all'utilizzatore che costituiscono illecito penale le condotte consistenti nella illecita duplicazione o riproduzione di software ai sensi della legge sul diritto d'autore n. 633/41 come novellata.

UTILIZZO SUPPORTI MAGNETICI E DATI

1. È fatto obbligo conservare, custodire e controllare i supporti informatici removibili contenenti dati, informazioni, notizie o immagini di attinenza scolastica, affinché nessun soggetto terzo ne prenda visione o possesso.
2. Qualsiasi file estraneo all'attività lavorativa o non espressamente autorizzato, non può, nemmeno in via transitoria, essere salvato sul pc in uso del dipendente.
3. Tutti i file che fanno parte dell'attività lavorativa, devono essere salvati nelle unità di rete messe a disposizione e mai localmente sul pc.
4. Gli accessi cartelle di rete che esulano dal profilo personale e l'accesso a nuove cartelle condivise devono essere richieste alla direzione che informerà l'amministrazione di sistema

UTILIZZO RETE INTERNA

1. La rete interna, istituita appositamente per permettere collegamenti funzionali tra utenti che prestano servizio all'interno della struttura scolastica, non può esser utilizzata per scopi diversi da quelli ai quali è destinata.
2. Qualora nella rete interna debbano circolare dati, notizie ed informazioni aziendali, deve essere premura di ciascun dipendente preservare gli stessi dalla conoscibilità di terzi soggetti non espressamente autorizzati ad aver notizia di tali dati.

UTILIZZO RETE ESTERNA INTERNET

3. È fatto divieto memorizzare dalla rete documenti, file o dati comunque non attinenti lo svolgimento delle attività aziendali, in particolare:
    a. è vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
    b. non è permessa la partecipazione, per motivi non professionali, a Forum, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest book anche utilizzando pseudonimi (o nicknames) potendo
    c. esporre a rischi di sicurezza la rete aziendale;
4. Si rende nota l'attivazione di filtri idonei ad evitare navigazioni in siti non correlati all'attività lavorativa. Le categorie bloccate dal sistema sono:

GIOCHI E GIOCHI D'AZZARDO
IMMAGINI CON ABUSO DI MINORI
PEER-TO PEER
PORNOGRAFIA E SESSUALITÀ ESPLICITA
SOCIAL NETWORKING

La black-list con la definizione dei siti viene periodicamente aggiornata dal software di protezione PANDA CLOUD PROTECTION PLUS. Eventuali categorie aggiuntive di protezione possono essere richieste

5. Si rende noto che il CFP Vantini ha attivato sistemi di monitoraggio della navigazione secondo le previsioni di cui al Provvedimento del Garante in materia di trattamento dati personali, Provvedimento del 1 marzo 2007, effettuando monitoraggio generalizzato ed anonimo dei log di connessione individuando per ogni singolo dispositivo i siti visitati con data, ora, dimensione traffico effettuato.

UTILIZZO FAX

1. Si raccomanda di non lasciare documenti incustoditi presso le postazioni di fax all'atto dell'invio.
2. Qualora il dipendente sia prossimo a ricevere atti contenenti dati o informazioni riservate via fax, avrà cura di monitorare la postazione fax e preservare – limitatamente alle oggettive possibilità – la conoscibilità di tali dati o informazioni, da parte di terzi non autorizzati.

UTILIZZO POSTA ELETTRONICA

1. Le caselle di posta elettronica date in uso sono destinate ad un utilizzo di tipo scolastico. Si rappresenta che:
   a. non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica, o che costituiscano comunque condotta illecita;
   b. non è consentito l'utilizzo dell'indirizzo di posta elettronica scolastica per la partecipazione a dibattiti, Forum, newsletter o mail-list, non attinenti l'attività lavorativa.
2. È fatto divieto di divulgare le notizie, i dati e qualsiasi altra informazione appresa in occasione della ricezione o invio di posta elettronica, in quanto coperte dal segreto professionale cui sono tenuti i dipendenti in ottemperanza agli obblighi di fedeltà e correttezza.
3. È obbligatorio controllare i file allegati di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).
4. È vietato inviare catene telematiche. Se si dovessero ricevere messaggi di tale tipo, si deve procedere alla cancellazione immediata.
5. Per quanto riguarda i soggetti non dipendenti scolastici si sottolinea che essere titolare di un indirizzo mail aziendale non comporta alcun rapporto di subordinazione ma si rende necessaria per l'accesso ai servizi aziendali e/o allo svolgimento dell'incarico.

GESTIONE, CONSERVAZIONE E CONTROLLO DEI DATI INFORMATICI

1. È fatto divieto applicare sistemi di crittografia, codificazione e simili ai dati aziendali.
2. È fatto divieto rimuovere dalle cartelle di rete dati utili per l'azienda alla cessazione del proprio rapporto.

SEGRETO PROFESSIONALE

1. L'utente non può divulgare, pubblicare o comunicare in alcun modo a terzi, direttamente o indirettamente, in toto o in parte, le informazioni apprese in occasione dello svolgimento delle mansioni per le quali è stato assunto dalla società, né potrà usarle, sfruttarle o disporne in proprio o tramite terzi.

2. Gli obblighi del personale previsti in questo capo non termineranno all'atto di cessazione del rapporto di lavoro, se non in riferimento a quelle specifiche parti delle informazioni che il dipendente possa dimostrare che erano già di pubblico dominio al momento della conclusione del rapporto, o che lo sono diventate in seguito per fatto a lui non imputabile.

RISERVATEZZA DEI DATI

1. Premesso che per «Informazioni Riservate» si intendono tutte le informazioni di qualsivoglia natura riferite o apprese in occasione dello svolgimento di mansioni per le quali il soggetto è stato assunto dalla società, il dipendente si impegna a considerare le Informazioni Riservate come strettamente private e riservate e ad adottare tutte le misure necessarie per non pregiudicare la riservatezza di tali informazioni;
2. Il dipendente si impegna ad utilizzare le Informazioni Riservate unicamente allo scopo di effettuare lo svolgimento dell'attività cui è preposto e di conseguenza a non usare tali informazioni in alcun modo che arrechi danno alla società, né per alcun altro scopo di qualsiasi natura;
3. Gli impegni di cui al presente capo non proibiscono di comunicare Informazioni Riservate:
    a. alla Direzione, soci, avvocati, revisori, banche o altri nostri consulenti ai quali la conoscenza di tali Informazioni è necessaria al fine dell'espletamento di attività funzionali all'ente;
    b. soggetti diversi da quelli specificati alla precedente lettera a., qualora ciò sia stato autorizzato dall'ente;
4. L'obbligo di riservatezza non opera in caso di Informazioni Riservate:
    a. che al momento in cui vengono rese note siano di pubblico dominio;
    b. che diventino di pubblico dominio dopo essere state rese note per causa non imputabile al dipendente;
5. L'impegno di riservatezza di cui al presente capo si protrarrà anche dopo la cessazione del rapporto di lavoro e sino a quando le informazioni in oggetto non saranno rese di pubblico dominio.

APPLICAZIONE ED INTERPRETAZIONE DEL PRESENTE REGOLAMENTO

1. Per qualsiasi dubbio relativo all'applicazione pratica o all'interpretazione del presente regolamento, il personale può rivolgersi alla direzione.

DISCIPLINA DEROGHE E MODIFICHE DEL PRESENTE REGOLAMENTO

1. Qualora al presente regolamento la società intenda apporre modifiche, queste saranno applicate dandone conoscenza immediata al personale.
2. Deroghe o modifiche di uno o più punti del presente regolamento, non rendono invalidi gli altri punti.

MEP SERVICE SRL

(un amministratore)

(Pasini Enrico)