I S T I T U T O T E C N I C O T E C N O L O G I C O S T A T A L E
" A l e s s a n d r o V O L T A "
Costruzioni, Ambiente e Territorio – Informatica e Telecomunicazioni – Elettronica ed Elettrotecnica
Meccanica, Meccatronica ed Energia

Protocollo e firma come da segnatura digitale

Trieste, 30.11.2018

Circolare n. 184

Al personale Docente e ATA
in servizio nell'Istituto

OGGETTO: INDICAZIONI REGOLAMENTARI AI DIPENDENTI - *utilizzo in sicurezza della rete e dei dispositivi e servizi informatici*

Ai sensi della normativa vigente (D.L.gs 196/2003 e GDPR – Reg. n. 2016/679) che impone precise procedure per il trattamento dei dati, si forniscono di seguito le INDICAZIONI REGOLAMENTARI di cui all'oggetto con la richiesta di attenta lettura e scrupolosa attuazione.

La Dirigente Scolastica

Clementina Frescura

INDICAZIONI REGOLAMENTARI AI DIPENDENTI
utilizzo in sicurezza della rete e dei dispositivi e servizi informatici

INDICE

Premessa _____ **pag.2**

Utilizzo di Personal Computer, Tablet, SmartPhone e similari _____ **pag.2**

Utilizzo della Rete di Istituto (cablata e Wireless) _____ **pag.3**

Gestione delle Password e delle credenziali di accesso in genere _____ **pag.4**

Uso della posta elettronica _____ **pag.4**

Uso della rete Internet e dei relativi servizi _____ **pag. 5**

Controllo dell'attività degli studenti _____ **pag. 5**

Non osservanza del Regolamento _____ **pag. 5**

Aggiornamento e revisione _____ **pag. 5**

Premessa

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet dai Personal Computer e dai dispositivi personali, espone anche il nostro Istituto ai rischi di un coinvolgimento sia patrimoniale sia penale, creando potenziali problematiche alla sicurezza dell'Istituto (sicurezza informatica, integrità dei dati, privacy).
Premesso quindi che l'utilizzo delle risorse informatiche e telematiche del nostro Istituto deve sempre ispirarsi al principio della diligenza e correttezza, la scrivente ritiene necessario fornire alcune Indicazioni Regolamentari cui i dipendenti, Docenti e Personale ATA, dovranno attenersi al fine di evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati.
Il presente regolamento si applica per tutti i seguenti casi:

- utilizzo di tutti i dispositivi informatici di istituto (fissi e mobili) dentro e fuori l'istituto;
- utilizzo di tutti i dispositivi informatici personali utilizzati per attività di lavoro;
- utilizzi della rete di istituto per accesso INTRANET ed INTERNET sia in modalità wireless che cablata;
- utilizzi dei Servizi web ed informatici, anche dall'esterno dell'Istituto, erogati direttamente o indirettamente dall'Istituto (ad es. sito-web, registro elettronico, posta elettronica, similari);
- altri utilizzi connessi, derivati o assimilabili a quelli precedenti.

Utilizzo di Personal Computer, Tablet, SmartPhone e similari

I Personal Computer dell'Istituto, affidati e/o utilizzati a scuola e/o a casa dal dipendente/collaboratore, sono uno **strumento esclusivamente di lavoro:** ogni utilizzo non inerente

all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. La medesima osservazione è valida per ogni altro dispositivo elettronico dell'Istituto similare o assimilabile (Tablet, Smart-Phone, etc.). **I dispositivi personali utilizzati ai fini lavorativi (per esempio per accesso al registro elettronico) sono da considerarsi "strumenti di lavoro" e conseguentemente soggetti al presente regolamento. Ogni difformità dei dispositivi personali utilizzati come strumento di lavoro rispetto alle indicazioni del presente regolamento può comportare un incremento del livello di rischio rispetto al quale il proprietario del dispositivo sarà considerato responsabile.**
L'accesso al dispositivo, alla Rete di Istituto e ad Internet ed eventualmente ad altri servizi (es. Registro Elettronico, sito-web, etc.) è protetto da credenziali di autenticazione (user-name e password) e/o da certificati di autenticazione equivalenti. **Tutte le credenziali devono essere custodite con la massima diligenza e non divulgate per nessuna ragione.** Non è consentita l'attivazione della password di accensione (bios o equivalente) senza preventiva autorizzazione da parte del Responsabile.
Il custode generale delle credenziali (l'Amministratore di Rete**,** direttamente o indirettamente) per l'espletamento delle sue funzioni, ha la facoltà in qualunque momento di accedere ai dati trattati da ciascuno per congrui motivi professionali.
Non è consentito installare autonomamente programmi provenienti dall'esterno in quanto detta operazione presuppone l'autorizzazione esplicita del Responsabile, in quanto sussiste il grave pericolo di portare Virus informatici (e similari) e di alterare la stabilità dell'elaboratore e/o della Rete.
Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dal responsabile dei sistemi informatici. L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema, può esporre l'Istituto a gravi responsabilità civili ed anche penali in caso di violazione 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. Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC; anche in questo caso si rende necessaria l'autorizzazione esplicita del Responsabile.
Ogni dispositivo deve essere spento, da quanti lo stanno utilizzando, prima di lasciare gli uffici/aule/laboratori o in caso di assenze prolungate dal luogo/aula di lavoro. Lasciare un dispositivo incustodito (eventualmente connesso alla rete) può essere causa di utilizzo non autorizzato da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. In ogni caso, su ogni dispositivo, deve essere attivata l'apposita modalità di blocco (o equivalente) che richiede la password per sblocco ed utilizzo.
Non è consentita l'installazione sul PC o tablet o personal computer, dato in uso dalla scuola di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio modem, Access Point, etc.), se non con l'autorizzazione espressa del Responsabile.
Ogni utente deve prestare la massima attenzione ai supporti di memorizzazione di origine esterna (es. Memorie USB), avvertendo immediatamente il Responsabile nel caso in cui vengano rilevati virus.

Utilizzo della Rete di Istituto (cablata e Wireless)

L'accesso alla rete di Istituto, sia in modalità wireless che cablata, è consentito esclusivamente per attività strettamente lavorative e soltanto per gli utenti già in possesso di credenziali di autenticazione fornite dal Responsabile.
Le unità di rete (così come gli altri spazi in rete di memorizzazione) 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. Sulle stesse, vengono svolte regolari attività di controllo, amministrazione e backup.

Le password d'ingresso alla rete ed ai servizi sono segrete, personali e riservate. È assolutamente proibito entrare nella rete e nei servizi con altri nomi utente.
Il Responsabile 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.
Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante.

Gestione delle Password e delle credenziali di accesso in genere

Le credenziali di accesso ai dispositivi informatici, alla Rete ed ai Servizi sono previste ed attribuite dal Responsabile.
È necessario procedere alla modifica della password al primo utilizzo e, successivamente, almeno ogni tre mesi. Le password devono essere formate da lettere (maiuscole o minuscole) e numeri ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema; è suggerito di includere nelle password almeno un carattere "speciale". In ogni caso le password devono essere composte da almeno otto caratteri e non devono contenere riferimenti agevolmente riconducibili all'incaricato (es. Nome, cognome, data di nascita, codice fiscale, etc.). **La password deve essere immediatamente sostituita, dandone comunicazione al Responsabile, nel caso si sospetti che la stessa abbia perso la segretezza.**
Qualora l'utente venisse a conoscenza delle password di altro utente (o di una qualsiasi altra credenziale di accesso), è tenuto a darne immediata notizia al Responsabile.
In fase di digitazione delle credenziali su qualsiasi dispositivo ogni utente è tenuto a prestare la massima attenzione al fine di valutare la sicurezza dell'ambiente circostante e della singola situazione specifica rispetto al rischio di frode visiva delle credenziali da parte di terzi; le credenziali non dovranno mai essere digitate su alcun dispositivo in caso di sospetto o rischio elevato di frode visiva.
In generale, le credenziali di accesso sono strettamente personali e riservate; è fatto divieto assoluto di scrivere e/o memorizzare qualsiasi credenziale di accesso. Le password sono segrete, personali e riservate. È assolutamente proibito accedere ai macchine, rete e servizi con credenziali non proprie.

Uso della posta elettronica

La casella di posta elettronica di Istituto assegnata all'utente è uno strumento di lavoro.
A partire dal 20.12.2018 l'indirizzo di posta elettronica assegnato ad ogni dipendente, cognome.nome@volta.ts.it, costituirà l'unica modalità di comunicazione di posta elettronica tra scuola e dipendente. Non saranno pertanto prese in considerazioni comunicazioni email provenienti da indirizzi personali. Al fine di organizzare tale modalità comunicativa i dipendenti dovranno recarsi dall'Assistente Tecnico Informatico per il ritiro delle credenziali di accesso.
Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
È fatto divieto di utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list salvo diversa ed esplicita autorizzazione.
È buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni informali tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.
La documentazione elettronica che contiene dati sensibili o comunque informazioni potenzialmente sensibili, delicate o riservate non può essere comunicata all'esterno senza preventiva autorizzazione della DS.

Per la trasmissione di file all'interno dell'Istituto è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati.
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 altre fonti non conosciuti).
È vietato inviare catene telematiche (o di Sant'Antonio). Se si dovessero ricevere messaggi di tale tipo, li si deve comunicare immediatamente al Responsabile. Non si devono in alcun caso attivare gli allegati di tali messaggi.

Uso della rete Internet e dei relativi servizi

Il dispositivi abilitati alla navigazione in Internet ed all'utilizzo dei Servizi web di Istituto costituiscono uno strumento necessario allo svolgimento della propria attività lavorativa. **È assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.**
È proibito all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dal Responsabile. È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dalla Direzione e con il rispetto delle normali procedure di acquisto.
È da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa. È vietata la partecipazione a Forum non professionali, l'utilizzo di chat (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books e similari anche utilizzando pseudonimi (o nicknames).

Controllo dell'attività degli studenti

I Docenti di Area Tecnica, in occasione dell'utilizzo dei Laboratori Informatici da parte delle classi, avranno cura di descrivere agli studenti le presenti Indicazioni Regolamentari per quanto attiene ai possibili aspetti di loro coinvolgimento diretto: Utilizzo della Rete di Istituto (cablata e Wireless) e Uso della rete Internet e dei relativi servizi.
Si richiede ai Docenti e per quanto possibile e di eventuale competenza, al Personale ATA di vigilare scrupolosamente affinché anche gli studenti si attengano scrupolosamente alle Indicazioni Regolamentari che possono essere loro riferibili.
Ogni comportamento degli studenti, difforme da quanto indicato nel presente testo, dovrà essere prontamente segnalato alla Dirigenza per i conseguenti provvedimenti.

Non osservanza delle Indicazioni Regolamentari fornite dalla dirigenza scolastica

Il mancato rispetto o la violazione delle presenti Indicazioni Regolamentari è perseguibile con provvedimenti disciplinari nonché con le eventuali azioni civili e penali.

Aggiornamento e revisione

Tutti i dipendenti possono proporre, quando ritenuto necessario, integrazioni al presente testo. Le proposte verranno esaminate dalla Dirigenza.
Le presenti Indicazioni sono soggette ad aggiornamento e revisione.

Firmato digitalmente

La Dirigente Scolastica

Clementina Frescura