REGOLAMENTI E POLICY
PER LA “SICUREZZA INFORMATICA”

8° Istituto Comprensivo “ELIO VITTORINI”

Via Regia Corte n°15

96100 Siracusa

INTRODUZIONE

La rapidità con cui le nuove tecnologie stanno entrando a far parte ogni giorno sempre più della quotidianità delle nostre vite, attraverso la rete Internet ed il Web, costituisce una seria minaccia in coinvolgimenti patrimoniali, penali e di pirateria informatica, minando la sicurezza dell'Istituto ed esponendo tutti i suoi membri a rischi e sanzioni notevoli.

Le norme inerenti l'uso delle tecnologie informatiche, sono da sempre legate ai principi della prudenza, della correttezza e della consapevolezza nell'utilizzo degli stessi, ma il nostro Istituto, nonostante questo, ha predisposto il seguente regolamento, sulle linee guida di quello europeo per promuovere, incentivare ed attuare in ogni sua forma la "cultura della Sicurezza" e tutelare il trattamento dei dati personali, onde incorrere in comportamenti inconsapevoli e sanzionabili a riguardo del loro utilizzo.

REGOLAMENTO "SICUREZZA INFORMATICA"

A riguardo l'elaborazione di tale codice comportamentale di Sicurezza Informatica disciplina le modalità e le norme per l'utilizzo consapevole e corretto degli apparecchi informatici dai lavoratori della Scuola ed indica agli stessi, le azioni consentite per preservare e tutelare la Sicurezza Informatica di tutta la Scuola e dei suoi studenti. Il regolamento tiene presente nelle sue norme delle indicazioni a riguardo previste dal contratto di lavoro e nello specifico del "GDPR" adottato dal 25 maggio del 2018.

A seguire una tabella riassuntiva relativa alle norme ed alle regole condivise all'interno dell'Istituto per garantire, in ogni sua parte l'attuazione dello stesso nelle situazioni che giornalmente le figure operanti della Scuola, devono fronteggiare.

IL REGOLAMENTO DI "SICUREZZA INFORMATICA" NELLE SUE PARTI ESSENZIALI		
1.Utilizzo del Personal Computer	**2.Utilizzo della rete Vittorini-SR**	**3.Utilizzo della Password d'Istituto**
4.Utilizzo dei dispositivi mobili ed USB di Istituto	**5.Utilizzo della posta elettronica**	**6.Utilizzo della Rete Internet**
7.Utilizzo protezione antivirus	**8.Rispetto delle norme in materia di Privacy**	**9.Sanzioni per non osservanza del regolamento di Sicurezza Informatica**

1.- UTILIZZO DEL PERSONAL COMPUTER

1.1 Il personale della Scuola è responsabile di tutti gli apparecchi informatici su cui lavora e che ha ricevuto in carico.

La destinazione degli stessi è strettamente collegata alla mansione che svolge nell'Istituto, pertanto deve essere consapevole che ogni utilizzo degli stessi, non inerente il proprio lavoro, può creare disservizi, spese per la manutenzione ed essere motivo di problematiche in campo di sicurezza.

1.2 L'attivazione della password è consentita solo su autorizzazione dell'8°I. C. Elio Vittorini di Siracusa.

1.3 Gli utenti non possono modificare le caratteristiche hardware e software degli strumenti informatici utilizzati, tranne previa autorizzazione formalizzata dell'8°I.C. Elio Vittorini di Siracusa.

1.4 I computer presenti in ogni stanza/ufficio/classe/sezione dell'Istituto, devono essere chiusi al termine delle attività lavorative, d'insegnamento e di studio e alla

chiusura della Scuola e durante altre attività che non ne richiedano l'utilizzo.

1.5 Non si possono archiviare e conservare informazioni e dati, non inerenti quelli che riguardano le attività lavorative che si svolgono e che sono previste dalla normativa a riguardo.

1.6 Al termine dell'anno scolastico in corso è consigliabile cancellare dalla memoria del computer, file vecchi, obsoleti o ritenuti inutili, con particolare riguardo a quelli duplicati, per il pratico e valido principio della "non eccedenza".

1.7 E' severamente vietato l'utilizzo di dispositivi di memoria removibili, per la memorizzazione o la trasmissione su computer differenti da quello in uso, di dati sensibili e personali. L'utente finale formalmente designato, avrà il compito di effettuare con cadenza periodica, i salvataggi dei dati indispensabili ed importanti per l'istituzione, su idonei supporti magnetici, in rete e la conservazione idonea degli stessi per i tempi necessari e comunque previsti dalla legge.

1.8 Sui computer non si possono istallare programmi non previsti dall'istituzione, salvo autorizzazione della stessa.

1.9 E' vietata la riproduzione e la duplicazione dei programmi informatici presenti nei sistemi informatizzati utilizzati, ai sensi della legge n°128 del 21 maggio 2004.

1.10 I tecnici incaricati della manutenzione e dei controlli periodici sui sistemi informatici, saranno autorizzati a eliminare e rimuovere applicazioni, programmi e file ritenuti non idonei al funzionamento degli stessi o considerati pericolosi per la sicurezza informatica e non solo per le strumentazioni, ma anche per le unità di rete.

2.- UTILIZZO DELLA RETE VITTORINI – SR

2.1 L'utilizzo della rete istituzionale è limitato da password; le credenziali con usarname "VITTORINI" sono fornite ai lavoratori della Scuola esclusivamente su autorizzazione, dai preposti del D.S. e del D.S.G.A. per lo svolgimento delle mansioni a cui sono destinati.

2.2 La rete istituzionale non può essere utilizzata per fini non inerenti la propria attività lavorativa o non espressamente autorizzati.

2.3 E' vietato, connettere in rete attività e situazioni inerenti l'Istituto, previa esplicita e formale autorizzazione dell'istituzione

2.4 E' vietato condividere file e cartelle in rete provviste e non di password, salvo esplicita e formale autorizzazione dell'istituzione.

3.- GESTIONE DELLE PASSWORD

3.1 La password di accesso alla rete di istituto, ai programmi, ai software installati, ed all'accesso alla banca dati per il personale preposto, è attribuita dall'istituzione scolastica 8°Istituto Comprensivo Elio Vittorini di Siracusa, nella figura del D.S. del D.S.G.A. e dei preposti incaricati.

3.2 L'utente che ha ricevuto la password è tenuto a conservarla in segretezza e non diffonderla previa esplicita e formale autorizzazione dell'Istituzione.

3.3 Il personale autorizzato ad accedere con password ai sistemi informatici scolastici, deve obbligatoriamente scollegarsi ed uscire da ogni area riservata, se costretto ad allontanarsi per motivi di lavoro o personali e se consapevole di lasciare incustodita la sua postazione e comunque non in grado di poterla controllare, durante la sua momentanea assenza.

Ciò potrebbe causare, la visione o la diffusione di dati sensibili a soggetti non

autorizzati o l'utilizzo a terzi per usi non consentiti, della strumentazione informatica senza che vi sia modo di provarne l'uso inappropriato ed indebito, successivamente.

3.4 In caso di clonazione o furto o sospetto di eventuale perdita di segretezza della password d'accesso, bisognerà intervenire con immediata segnalazione per poi procedere con l'impostazione di una nuova password.

4.- UTILIZZO DEI DISPOSITIVI MOBILI E USB D'ISTITUTO


4.1 Ogni lavoratore ha la responsabilità dei device mobili e delle USB, che gli sono state affidate, per cui ne risponde in qualsiasi momento fino a riconsegna.

4.2 Per i computer portatili, tablet e per tutti i device mobili si applicano le stesse regole utilizzate per i computer fissi.

I portatili e i device mobili devono essere riconsegnati senza file o App installate successivamente alla consegna e senza codici di blocco o password d'accesso.

4.3 Gli strumenti mobili informatici, che escono dalla Scuola, devono essere custoditi nelle migliori condizioni e riconsegnati integri e funzionanti.

4.4 Ogni dispositivo portatile non deve restare mai incustodito e devono essere installati e conservati applicativi e file necessari ed utili alle attività comunemente svolte nel proprio ambito lavorativo.

4.5 Utilizzare i dispositivi mobili unicamente con la rete scolastica VITTORINI e farne uso esclusivamente personale.

4.6 Disconnettere i device portatili dalla rete scolastica, al termine della sessione di lavoro ed utilizzare la password in modo esclusivo, senza memorizzarla, sui portatili o sui tablet adoperati.

4.7 Effettuare periodicamente l'antivirus e verificare gli aggiornamenti disponibili,

quando si è collegati correttamente con una certa periodicità, nonostante quelli attivati dal sistema.

4.8 Non utilizzare USB personali o non fornite dalla scuola, effettuando l'antivirus prima di attivarle e scollegandole al termine di ogni sessione di lavoro, nella modalità corretta.

5.- UTILIZZO DELLA POSTA ELETTRONICA

5.1 Tutti i lavoratori dell'Istituto, potranno usufruire della posta elettronica @vittorini.edu.it fino al termine del contatto di lavoro presso l'Istituto.

5.2 La posta elettronica d'Istituto assegnata ai lavoratori è indispensabile proprio per i compiti che si svolgono, pertanto gli stessi sono responsabili del suo uso che è finalizzato a modalità corrette e precise per le quali ogni dipendente ne viene fornito.

5.3 Nonostante le segnalazioni sulla posta in entrata ed in uscita, che vengono fornite puntualmente dalla piattaforma Workspace che attribuisce ad ogni dipendente la casella di posta elettronica, in caso di mittenti esterni sconosciuti è consigliabile cestinare i messaggi senza nemmeno aprirli e si consiglia di attuare la stessa procedura per file sospetti con estensioni diverse dalle più comunemente usate.

5.4 Non aprire, ne' rispondere a mail di diffusione capillare e non memorizzare indirizzi di indubbia o sconosciuta provenienza senza effettuare eventuali verifiche.

5.5 Per allegati pesanti utilizzare i formati zip, rar, e jpg.

5.6 Non iscriversi a mailing list esterne senza le adeguate ed indispensabili verifiche e senza autorizzazione dell'istituzione scolastica.

5.7 La casella elettronica fornita ad ogni lavoratore deve essere tenuta sempre in

ordine e priva di allegati inutili, ingombranti ed obsoleti e non deve mai essere utilizzata per alcun motivo, per motivi personali, non attinenti alle mansioni che si svolgono.

5.8 Per la trasmissione di allegati, file e documenti, si consiglia di restare al di sotto dei 70 MB.

6.- UTILIZZO DELLA RETE INTERNET

6.1 L'abilitazione all'utilizzo della rete internet d'Istituto è concessa a tutti i dipendenti in servizio che ne necessitano per la propria attività lavorativa e su autorizzazione.

6.2 I computer ed i PC sono indispensabile strumento lavorativo, per cui vengono forniti con connessione alla rete internet a tutti i lavoratori che ne necessitano.

6.3 Non è consentita la navigazione sul web per motivi strettamente personali o non inerenti all'attività lavorativa che si svolge, utilizzando la rete internet d'Istituto.

6.4 Non si possono scaricare App e software gratuiti o a pagamento da siti internet senza consenso e formale autorizzazione dell'Istituto.

6.5 E' fatto divieto di partecipare a forum, corsi, videoconferenze, seminari e workshop, ne colloquiare in chat sulla rete internet o con l'account istituzionale senza formale richiesta ed autorizzazione dell'Istituto.

7.- UTILIZZO PROTEZIONE ANTIVIRUS

7.1 Ogni lavoratore della scuola deve fare uso responsabile degli strumenti informatici affidati, adottando una navigazione sul web responsabile e legale. Ciò ridurrà eventuali pericoli di attacchi informatici e la trasmissione di virus, che

potrebbero seriamente compromettere la tutela dei dati sensibili e l'operatività degli strumenti informatici.

7.2 I lavoratori sono tenuti a verificare che la protezione antivirus sia regolarmente installata e funzionante sugli strumenti informatici che utilizza.

7.3 La scansione intelligente del sistema deve essere regolarmente controllata e devono essere effettuati gli aggiornamenti richiesti dal sistema, con le adeguate procedure.

7.4 Spam, virus e malware non eliminati dalla protezione antivirus in uso, devono essere isolati, mai aperti ed eliminati o segnalati immediatamente ai preposti incaricati dal D.S.

7.5 Per la condivisione, l'archiviazione e la conservazione di ogni tipologia di file e di cartelle contenenti dati sensibili e personali è fatto divieto di utilizzo di archivi magnetici mobili ed USB soprattutto se esterni all'Istituto. In caso di indispensabile ed irrinunciabile utilizzo degli stessi è obbligo effettuare scansioni antivirus, prima di utilizzarli e collegarli alla strumentazione informatica dell'Istituto.

8.- RISPETTO DELLE NORME IN MATERIA DI PRIVACY

8.1 I dipendenti dell'Istituto dovranno attenersi scrupolosamente al regolamento UE 2016/679 GDPR relativo alla protezione delle persone fisiche con riguardo al trattamento ed alla libera circolazione dei dati personali.

In questo caso con maggior cautela e precauzione nel diffondere, lavorare, utilizzare e condividere dati personali, utilizzando gli strumenti informatici.

9.- SANZIONI PER NON OSSERVANZA DEL REGOLAMENTO DI SICUREZZA INFORMATICA

9.1 Per garantire un uso consapevole, corretto, sicuro ed efficace della dotazione

informatica dell'Istituto, il seguente regolamento e le norme in esso contenute potranno sicuramente facilitare l'acquisizione di comportamenti e procedure che garantiranno la sicurezza di tutte le figure operanti nella scuola e soprattutto quella degli studenti, il cui approccio al mondo della "rete" mediato dal personale e dai docenti in servizio, sarà sicuramente il più corretto possibile, al riparo dai rischi e dalla pirateria informatica che rappresenta una seria minaccia e l'occasione per gli stessi di incappare in contenuti inappropriati, illeciti e in situazioni caratterizzate da comportamenti offensivi e scorretti.

Pertanto il mancato rispetto o la violazione delle regole contenute nel presente regolamento, sarà perseguibile con provvedimenti disciplinari ed azioni civili e penali previsti dalla normativa a riguardo.

(art.171-ter art.248/00 art.547 art.594 e 595 art.600-ter e seg. art.615-ter art.615-quater art.615-quinques art.617-quater art.617-quinquies art.617-sexies art.613-bis art.640 e 640 ter)

L'Animatore Digitale

Assunta Papa