Titolo	**E-SAFETY**
Tipo di documento	Procedura Operativa
Emesso da	Safeguarding Staff
Data di emissione	20/03/2024
N° Allegati	0
Stato	Attivo

Redatto	Safeguarding Staff	Nicola Gotti – Responsabile IT
Verificato	Luca Radici	Direttore Scolastico
Approvato		

1. INTRODUZIONE

L'ambiente scolastico è il luogo privilegiato nel quale poter attuare un percorso di crescita umana, relazionale, didattica e cognitiva quotidiana. Oltre a vivere processi di apprendimento, i ragazzi hanno occasione di allargare le loro amicizie; questo significa anche doversi confrontare, a volte, con le difficoltà nel relazionarsi con i pari e saper gestire gli eventuali insuccessi.

Ne consegue che fattori come relazioni positive e un ambiente di apprendimento sereno influenzino la qualità della vita, nonché la percezione del benessere e della salute.

Autostima, felicità, gioia e tranquillità determinano in modo importante il benessere psicofisico degli Alunni e sono elementi indispensabili per garantire un percorso di crescita cognitiva ed emotiva armoniosa e serena.

La Scuola ha il compito fondamentale di garantire, insieme ai Genitori e ad altre agenzie educative del territorio, un processo di crescita e di apprendimento giusto ed equilibrato.

Ci si propone di:

- Fornire un ambiente sicuro e felice che incoraggi la crescita e l'apprendimento dei nostri studenti.
- Sensibilizzare tutti i dipendenti e i genitori sulle questioni relative alla sicurezza informatica
- Garantire una comunicazione efficace tra dipendenti e genitori in relazione a situazioni di rischio
- Essere chiari con tutti i soggetti coinvolti, compresi gli studenti, i genitori in merito alla suddetta policy

Per tale motivo, la Scuola predispone strategie educative e formative per promuovere il benessere di ogni Studente e ogni Studentessa ed arginare quindi situazioni che possano interferire in modo negativo sull'equilibrio degli Studenti.

La Scuola si impegna a garantire che gli alunni abbiano accesso alle migliori tecnologie digitali per migliorare il loro apprendimento e, in cambio, si aspetta che gli alunni accettino di essere utenti responsabili. È responsabilità della scuola garantire che la strumentazione sia sicura e conservata in modo consono, di modo da insegnare agli alunni come prendersi cura del proprio dispositivo e degli aspetti legati alla sicurezza elettronica durante l'utilizzo.
Qualsiasi tipo di violazione di sicurezza o rischio informatico va riportato al Docente o all'IT Manager della struttura scolastica.

2. I SISTEMI INFORMATICI AZIENDALI

Il materiale informatico affidato allo studente è a tutti gli effetti strumentazione di lavoro pertanto, tali strumenti vanno custoditi in modo appropriato e possono essere utilizzati solo per fini professionali (in relazione, ovviamente alle mansioni assegnate) e non per scopi personali, tanto meno per scopi illeciti; debbono essere prontamente segnalati all'azienda il furto, danneggiamento o smarrimento di tali strumenti.

La scuola verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole, l'integrità del proprio sistema informatico e la coerenza delle sue configurazioni e dei suoi archivi con le finalità aziendali. In questo contesto la scuola potrà per necessità di sicurezza aziendale o per esigenze di continuità della normale attività lavorativa, accedere agli archivi di corrispondenza elettronica o ai file di log riservati alla tracciatura degli eventi di connessione.

Utilizzo del computer

- è consentito installare programmi provenienti dall'esterno solo se espressamente autorizzati dalla scuola; non è consentito scaricare file dalla rete o contenuti in supporti magnetici e/o ottici non aventi alcuna attinenza con l'attività scolastica;
- non è consentito utilizzare strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti

informatici; non è consentita l'installazione sul proprio PC di mezzi di comunicazione propri (come ad esempio i modem);

- non è consentito condividere file, cartelle, hard disk o porzioni di questi del proprio computer, per accedere a servizi non autorizzati di peer to peer al fine di scaricare materiale elettronico tutelato dalle normative sul Diritto d'Autore (software, file audio, film, etc.);
- i Computer "stand alone" o in rete 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; la scuola si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza del sistema ovvero acquisiti o installati in violazione delle presenti istruzioni.

Utilizzo di internet

- non è consentito navigare in siti non attinenti allo svolgimento delle mansioni assegnate;
- a maggior ragione non è consentito navigare in siti che accolgono contenuti contrari alla morale e alle prescrizioni di Legge;
- non è inoltre consentito navigare in siti che possano rivelare una profilazione dell'individuo relativa a dati 'particolari' ai sensi del Reg. UE 2016/679: quindi siti la cui navigazione palesi elementi attinenti alla fede religiosa, alle opinioni politiche e sindacali dell'incaricato o le sue abitudini sessuali;
- non è consentita l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo casi direttamente autorizzati e con il rispetto delle normali procedure di acquisto;
- non è consentito lo scarico di software gratuiti trial, freeware e shareware prelevati da siti Internet, se non espressamente autorizzato;
- non è consentito lo scarico di materiale elettronico tutelato dalle normative sul Diritto d'Autore (software, file audio, film, etc.) né attraverso Internet né attraverso servizi di peer to peer;

- è vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività scolastica;
- non è permessa la partecipazione durante l'orario scolastico, a Forum e giochi in rete pubblica, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest book anche utilizzando pseudonimi (o nicknames);
- non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

Utilizzo del servizio di posta elettronica

Nel precisare che anche la posta elettronica è uno strumento di lavoro, si ritiene utile segnalare che:

- non è consentito utilizzare la posta elettronica (interna ed esterna) per motivi non attinenti allo svolgimento delle mansioni assegnate;
- 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;
- la posta elettronica diretta all'esterno della rete informatica aziendale può essere intercettata da estranei, e dunque, non deve essere usata per inviare informazioni, dati o documenti di lavoro "strettamente Riservati";
- non è consentito l'utilizzo dell'indirizzo di posta elettronica aziendale per la partecipazione a dibattiti, Forum o mail-list; solo in questo ultimo caso è possibile, previa autorizzazione per la verifica della validità dell'emittente, iscriversi a servizi di informazione strettamente inerenti all'attività aziendale;
- nel caso esista un dominio di proprietà aziendale (es.: nomeazienda.it) al quale sia collegato un servizio di posta e la relativa casella (es.: rossi@nomeazienda.it), non è consentito utilizzare web mail esterni, ovvero caselle di posta elettronica non appartenenti al dominio o ai domini aziendali salvo diversa ed esplicita autorizzazione.

3. MODALITÀ PER ELABORARE E CUSTODIRE LE PASSWORD

Le credenziali di autenticazione sono assolutamente personali e non cedibili, per nessuna ragione. Se si è in possesso di più credenziali di autenticazione, come nel caso delle utenze dei laboratori, fare attenzione ad accedere ai dati unicamente con la credenziale relativa alla lezione in oggetto. Elaborare le password seguendo le istruzioni sotto riportate.

SCELTA DELLE PASSWORD

Il metodo più semplice per l'accesso illecito a un sistema consiste nell'indovinare la password dell'utente legittimo. In molti casi sono stati procurati seri danni al sistema informativo a causa di un accesso protetto da password "deboli". La scelta di password "forti" è, quindi, parte essenziale della sicurezza informatica.

COSA NON FARE

- **NON** comunicare a nessuno la password. Lo scopo principale per cui usa una password è assicurare che nessun altro possa utilizzare le risorse di un utente o possa farlo a suo nome.
- **NON** scrivere la password in nessun posto in cui possa essere letta facilmente, soprattutto vicino al computer.
- Quando si immette la password **NON** far sbirciare a nessuno quello che si sta battendo sulla tastiera.
- **NON** scegliere password che si possano trovare in un dizionario. Su alcuni sistemi è possibile "provare" tutte le password contenute in un dizionario per vedere quale sia quella giusta.
- **NON** credere che usare parole straniere renderà più difficile il lavoro di scoperta, infatti chi vuole scoprire una password è dotato di molti dizionari delle più svariate lingue.
- **NON** usare il proprio nome utente. È la password più semplice da indovinare.
- **NON** usare password che possano in qualche modo essere legate all'utente stesso come, ad esempio, il nome, quello di un familiare, dei figli, del cane, date di nascita, numeri di telefono etc.

COSA FARE OBBLIGATORIAMENTE

- la password deve essere composta da almeno otto caratteri o, se il sistema non l'accetta, da un numero di caratteri pari a quello consentito dal sistema; è buona norma che, di questi caratteri, da un quarto alla metà siano di natura numerica;
- lo studente deve provvedere a modificare la password immediatamente, non appena la riceve per la prima volta, da chi amministra il sistema;
- la password deve essere modificata dallo studente almeno ogni 6 mesi;
- se il trattamento riguarda dati sensibili o giudiziari la password deve essere modificata almeno ogni tre mesi;

COSA FARE PRATICAMENTE
Utilizzare più di una parola e creare password lunghe

A volte è più semplice ricordare una frase completa di senso compiuto piuttosto che una parola complicata, e questa tecnica oltre a facilitare la memorizzazione migliora la sicurezza stessa della parola chiave: la lunghezza influisce sulle difficoltà di individuazione e ci consente di utilizzare lo "spazio" tra una parola e l'altra come ulteriore elemento da intercettare.
Inoltre è bene sapere che diversi strumenti di intercettazione presumono che le password non siano formate da più di 14 caratteri, e quindi, anche senza complessità, le password molto lunghe (da 14 a 128 caratteri) possono rappresentare un'ottima protezione contro possibili violazioni.

Utilizzare numeri e simboli al posto di caratteri

Non limitarsi alle sole lettere ma, dove possibile, utilizzare l'ampia gamma di minuscole/maiuscole, numeri e simboli a disposizione sulla propria tastiera:

- Caratteri minuscoli: a, b, c,...
- Caratteri maiuscoli: A, B, C,...
- Caratteri numerici: 0,1,2,3,4,5,6,7,8,9
- Caratteri non alfanumerici: (< > , .) ` ~ ! $ % ^ ; * - + = | \ { @ # } [/] : ; " '?

Non inserirli alla fine di una parola nota come ad es.:"computer987". In questo caso la password può essere identificata abbastanza facilmente: la parola "computer" è inclusa in molti dizionari contenenti nomi comuni e quindi dopo aver scoperto il nome restano solo 3 caratteri da identificare.

Al contrario, è sufficiente sostituire una o più lettere all'interno della parola con simboli che possono essere ricordati facilmente. Ad esempio si può provare a utilizzare "@"al posto di "A", "$"al posto di "S", zero (0) o la doppia parentesi () al posto di "O", e "3"al posto di "E": si tratta di trovare delle analogie che ci rendano familiare la sostituzione di lettere con simboli e numeri.

Con alcune sostituzioni si possono creare password riconoscibili per l'utente, ad esempio (es.: "Ve$tito di Mario"), già sufficientemente lunghe e estremamente difficili da identificare o decifrare.

Cercare di realizzare password utilizzando caratteri appartenenti a tutti i quattro gruppi rappresentati nella lista.

4. OBBLIGO DI NON LASCIARE INCUSTODITI E ACCESSIBILI GLI STRUMENTI ELETTRONICI, MENTRE È IN CORSO UNA SESSIONE DI LAVORO

Non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di lavoro. È necessario terminare la sessione al computer ogni volta che ci si deve allontanare, anche solo per cinque minuti effettuando un log out o mettendo in atto accorgimenti tali, per cui anche in quei cinque minuti il computer non resti:

- incustodito: può essere sufficiente che un collega rimanga nella stanza, durante l'assenza di chi sta lavorando con lo strumento elettronico, anche se la stanza rimane aperta;
- accessibile: può essere sufficiente chiudere a chiave la stanza, dove è situato lo strumento elettronico, durante l'assenza, anche se nella stessa non rimane nessuno.

Non si devono invece mai verificare situazioni in cui lo strumento elettronico venga lasciato attivo, durante una sessione di trattamento, senza che sia controllato da una persona autorizzata o senza che la stanza in cui è ubicato venga chiusa a chiave.

È possibile installare strumenti software specifici (es.: screen saver) che, trascorso un breve periodo di tempo predeterminato dall'utente in cui l'elaboratore resta inutilizzato, non consente più l'accesso all'elaboratore se non previa imputazione di password.

5. INCREMENTO DEL RISCHIO INFORMATICO FATTORI DI INCREMENTO DEL RISCHIO E COMPORTAMENTI DA EVITARE

- riutilizzo di unità removibili sconosciute;
- uso di software gratuito (trial, freeware o shareware) prelevato da siti Internet o in allegato a riviste o libri;
- collegamento in Internet con download di file eseguibili o documenti di testo da siti web o da siti FTP;
- collegamento in Internet e attivazione degli applets di Java o altri contenuti attivi;
- allegati di posta elettronica.

LINEE GUIDA PER LA PREVENZIONE DEI VIRUS

Un virus è un programma in grado di trasmettersi autonomamente e che può causare effetti dannosi. Alcuni virus si limitano a riprodursi senza ulteriori effetti, altri si limitano alla semplice visualizzazione di messaggi sul video, i più dannosi arrivano a distruggere tutto il contenuto del disco rigido.

Come prevenire i virus:

1. Usare solo programmi provenienti da fonti fidate

Copie sospette di programmi possono contenere virus o altro software dannoso. Ogni programma deve essere sottoposto alla scansione prima di essere installato. Non utilizzare programmi non autorizzati, con particolare riferimento ai videogiochi, che sono spesso utilizzati per veicolare virus.

2. Assicurare che il software antivirus sia aggiornato

La tempestività nell'azione di bonifica è essenziale per limitare i danni che un virus può causare; inoltre è vitale che il programma antivirus conosca gli ultimi aggiornamenti sulle "impronte digitali" dei nuovi virus. Questi file di identificativi sono rilasciati, di solito, con maggiore frequenza rispetto alle nuove versioni dei motori di ricerca dei virus. Mantenere costantemente aggiornati i sistemi di protezione in accordo con le policy di sicurezza e comportamento aziendali.

3. Non diffondere messaggi di provenienza dubbia

Se si ricevono messaggi che avvisano di un nuovo virus pericolosissimo, saranno da ignorare: le mail di questo tipo sono dette con terminologia anglosassone hoax (termine spesso tradotto in italiano con "bufala"), l'equivalente delle "leggende metropolitane" della rete. Questo è vero anche se il messaggio proviene dal suo migliore amico, dal suo capo o da un tecnico informatico. È vero anche e soprattutto se si fa riferimento a "una notizia proveniente dalla Microsoft" oppure dall'IBM (sono gli hoax più diffusi).

4. Non aprire link o allegati sospetti

Analogamente, tutti i messaggi che vi invitano a scaricare urgentemente un file o inserire le vostre credenziali bancarie per sbloccare il conto sono hoax. Questo tipo di richieste hanno spesso scopi molto simili a quelli dei virus, cioè utilizzare indebitamente le risorse informatiche e ottenere credenziali d'accesso. Si raccomanda di mostrare al Docente o all'IT Manager qualsiasi mail che si ritenga sospetta senza aprirla.

6. **Evitare la trasmissione di file eseguibili (.COM,. EXE,. OVL,. OVR) e di sistema (.SYS) tra computer in rete o via e-mail**

7. **Non utilizzare i server di rete come stazioni di lavoro**

Assicurarsi di non far partire accidentalmente il suo computer da un'unità removibile

Infatti se l'unità esterna fosse infettata, il virus si trasferirebbe nella memoria RAM e potrebbe espandersi ad altri files.

8. OBBLIGO DI RISERVATEZZA E CAUTELA NELLA COMUNICAZIONE A TERZI DI DATI E INFORMAZIONI

Anche informazioni di normale quotidianità scolastica o ritenute non riservate all'interno dell'interscambio tra studenti, assumono diversa importanza, e quindi necessitano di una maggiore tutela, se comunicate all'esterno a soggetti terzi. La salvaguardia delle informazioni e dei dati oltre ad essere un requisito fondamentale per la sicurezza del patrimonio informativo aziendale, è anche un espresso obbligo di legge nei confronti di qualsiasi soggetto definito "interessato". A fronte di tali motivazioni è importante ribadire la necessità di osservare ogni cautela nel trasferire all'esterno qualsiasi informazione proporzionalmente al loro contenuto e all'attendibilità dell'interlocutore.

SOCIAL ENGINEERING

Il social engineering è l'insieme delle tecniche psicologiche usate da chi vuole indurci ai propri scopi presentandosi personalmente presso di noi o contattandoci dall'esterno a mezzo telefono o posta elettronica. Gli obiettivi possono andare dalla raccolta di informazioni apparentemente innocue riguardanti l'azienda o la sua organizzazione e il personale che vi lavora, ma possono arrivare a raggiungere dati anche molto riservati.

Con l'ausilio di messaggi studiati o abili tecniche di persuasione l'aggressore può anche renderci complici inconsapevoli di azioni che andranno a suo beneficio come, ad esempio, l'acquisizione di informazioni o l'ottenimento della fiducia del personale, l'apertura di allegati infetti o la visita di un sito che contiene dialer o altro materiale pericoloso. Rispetto al social engineering via e-mail, uno dei principali problemi degli autori di virus è che molti utenti utilizzano strumenti di difesa aggiornati che non consentono l'esecuzione in automatico di applicativi e quindi non consentono l'attivazione di programmi dannosi.

Per scavalcare queste precauzioni e quindi lanciare il virus, c'è un modo molto semplice: indurre la vittima, tramite espedienti psicologici a fidarsi dell'allegato e quindi eseguirlo, o fidarsi del collegamento ad un sito web contenuto nel messaggio e quindi raggiungerlo. In questo senso l'aggressore potrebbe essere capace di sfruttare i nostri punti di debolezza redigendo abili messaggi che, inducendo fiducia o curiosità, riescono ad arrivare allo scopo.

E-MAIL PHISHING

Un altro scopo degli aggressori è indurre l'utente a fidarsi dell'intero contenuto di un messaggio di posta elettronica e quindi ottenere una fedele esecuzione delle istruzioni contenute: ad esempio, vengono inviate false comunicazioni e-mail aventi grafica, forma, autorevolezza e loghi ufficiali di enti noti, banche, intermediari finanziari, assicurazioni, etc., chiedendo informazioni attraverso moduli o link a pagine web debitamente camuffate. In questa modalità vengono richieste ad esempio password, numeri di carta di credito o altre informazioni riservate senza che in realtà la raccolta dati abbia nulla a che vedere con l'organismo ufficiale imitato. La vittima crede di comunicare con essi ma in realtà sta trasmettendo informazioni riservate all'aggressore.

Spesso queste tecniche sono abbinate tra loro e applicate più volte nel tempo sulla stessa vittima.

COSA FARE

- non fornire informazioni confidenziali al telefono o di persona a interlocutori non conosciuti;
- limitarsi a fornire informazioni a interlocutori noti e operanti con voi per disposizione aziendale, nei limiti dei contenuti afferenti all'ambito lavorativo a voi assegnato;
- diffidare di messaggi provenienti da fonte non conosciuta;
- non aprite messaggi provenienti da fonte non conosciuta contenenti allegati;
- non aprite messaggi contenenti allegati sospetti;
- non utilizzare mai link contenuti nel testo del messaggio perché possono essere facilmente falsificati; in questi casi si deve andare direttamente sul sito citato digitandone da capo il nome;

- non trasmettere mai alcuna informazione in risposta ad una richiesta proveniente da fonte sconosciuta;
- non trasmettere mai alcuna informazione in risposta ad una richiesta proveniente da fonti istituzionali o apparentemente conosciute (ad es.: banche) in quanto tali strutture non richiedono mai dati utilizzando questa modalità;
- in caso di dubbio è sempre preferibile verificare l'attendibilità delle richieste con i docenti e il team IT

9. CUSTODIA ED UTILIZZO DEI SUPPORTI RIMOVIBILI, CONTENENTI DATI PERSONALI

Una particolare attenzione deve essere dedicata ai supporti rimovibili (es. chiavette USB), contenenti dati particolari, nei seguenti termini:

- I supporti rimovibili (es. chiavette USB), contenenti dati particolari devono essere custoditi ed utilizzati in modo tale, da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti: è bene adottare archiviazioni in modo che vengano conservati in cassetti chiusi a chiave, durante il loro utilizzo, e successivamente formattati, quando è cessato lo scopo per cui i dati sono stati memorizzati su di essi.
- Una volta cessate le ragioni per la conservazione dei dati, i supporti non possono venire abbandonati. Si devono quindi cancellare i dati, se possibile, o arrivare addirittura a distruggere il supporto, se necessario.