ISTITUTO COMPRENSIVO STATALE
“ALESSANDRO MANZONI”
MARACALAGONIS BURCEI

LINEE GUIDA PER LA CYBERSICUREZZA

Approvato dal Consiglio d’Istituto in data.5 dicembre 2023delibera n.140

LINEE GUIDA PER LA CYBERSICUREZZA

In un'epoca in cui la tecnologia è una parte essenziale della nostra vita quotidiana, è fondamentale comprendere come proteggerci e navigare in modo sicuro nel mondo digitale. Questo vademecum è stato creato con l'obiettivo di fornire un insieme di regole e pratiche che promuovono un utilizzo sicuro e responsabile della tecnologia all'interno e al di fuori delle nostre mura scolastiche.

Le linee guida qui presentate non sono solo regole da seguire, ma rappresentano un impegno per la vostra sicurezza e per la tutela dei vostri dati personali. Attraverso l'adozione di comportamenti consapevoli e responsabili online, possiamo collettivamente contribuire a creare un ambiente digitale più sicuro e protetto per tutti noi.
Questo vademecum non è solo un elenco di regole statiche, ma piuttosto un documento dinamico che si adatterà alle nuove sfide e alle minacce emergenti nel mondo digitale. Sarà un punto di riferimento costante per promuovere la consapevolezza della cybersicurezza e garantire che tutti possano beneficiare in modo sicuro delle risorse digitali a disposizione.

Oltre a fornire linee guida chiare e pratiche, questo vademecum è anche un invito a una collaborazione attiva e alla condivisione di conoscenze. Le vostre domande, i vostri feedback e le vostre esperienze saranno parte integrante dell'evoluzione di queste linee guida.
Insieme, possiamo fare della nostra comunità scolastica un luogo in cui la tecnologia viene sfruttata in modo sicuro, responsabile e costruttivo.

Con questo vademecum per la cybersicurezza esploriamo il ruolo che la tecnologia gioca nell'ambito scolastico e approfondiamo l'importanza dei dispositivi elettronici nei moderni materiali didattici.
Mentre l'istruzione continua a evolversi, emerge una preoccupazione iniziale legata alla diffusione della nomofobia, un timore ossessivo legato alla privazione del cellulare.

I cellulari e le tecnologie rappresentano una sfida costante per il mondo educativo. La scuola ha sempre subito evoluzioni significative, ma attualmente, i cambiamenti avvengono a un ritmo rapido e incisivo, lasciando un'impronta immediata anziché manifestarsi nel corso di decenni, come in passato. Queste trasformazioni spesso generano reazioni intense e opinioni talvolta superficiali da parte di chi non è direttamente coinvolto nel contesto scolastico.

Lo smartphone e le tecnologie hanno da tempo un impatto significativo sull'ambiente didattico, suscitando numerosi interrogativi tra i docenti. Il rapporto tra la scuola e la tecnologia digitale è oggetto di discussione diffusa e l'utilizzo dei cellulari e della tecnologia è un tema su cui tutti sentono il dovere di esprimere il proprio punto di vista.

La tecnologia costituisce la più vasta risorsa attualmente disponibile, ma a volte può generare disagi, se non veri e propri problemi, a livello psicologico e educativo. Numerosi studi si occupano di questo argomento.

NOMOFOBIA

L'uso eccessivo del cellulare si è diffuso ampiamente, diventando un tema cruciale per il mondo dell'istruzione. Non basta adottare misure temporanee; semplicemente distrarre i giovani dagli schermi per un breve periodo non è la soluzione. Questo fenomeno è complesso e nasconde una forma di disagio che la scuola fatica ad affrontare. La Generazione Z si presenta come più determinata ma anche più fragile e stremata. L'ansia crescente sta diventando una caratteristica predominante nella vita di molti studenti.

La "nomofobia" è correlata a questa realtà. È un termine che descrive uno stato psicologico in cui alcuni individui provano una paura irrazionale di rimanere "isolati" o non poter usufruire del proprio cellulare, sia perché non lo hanno con sé sia perché si trovano in zone senza copertura.

La gestione del tempo dei giovani e l'affronto della nomofobia sono sfide a cui la scuola deve rispondere in modo efficace. Comprendere appieno le esperienze dei nostri ragazzi è essenziale per aiutarli a superare le sfide e garantire loro un percorso educativo (e di vita) senza le molteplici ansie legate alla paura di sentirsi soli.

INDICAZIONI PER I DOCENTI

1. **Insegnare la consapevolezza digitale:****

Educare gli studenti sulle minacce online e sensibilizzali sull'importanza di una condotta responsabile.

2. **Protezione delle informazioni personali:****

Insegnare a non condividere informazioni personali come nome completo, indirizzo, numero di telefono o informazioni sulla scuola su piattaforme
online.

3. **Password robuste:****

Aiutare gli studenti a creare password forti e insegnagli l'importanza di non condividerle con nessuno, tranne i genitori o gli insegnanti.

4. **Obbligo di utilizzare l’antivirus:****

Insegnare agli studenti l’uso del "software antivirus" per rilevare, prevenire e rimuovere software dannoso, malware e altre minacce informatiche che potrebbero compromettere l'integrità dei sistemi informatici.

Insegnare ai ragazzi/e a garantire che il software antivirus installato sui propri dispositivi sia aggiornato regolarmente.

4. Navigazione sicura:**

Guidare gli studenti a navigare solo su siti web sicuri e affidabili. Insegnare a riconoscere URL sospette e a evitare il clic su link non verificati.

5. Controllo della privacy sui social media:**

Informare gli studenti sull'importanza delle impostazioni della privacy sui social media e insegnare a controllare chi può vedere le loro informazioni personali.

6. Sensibilizzazione sul phishing:**

Spiegare cosa sono gli attacchi di phishing e come riconoscerli. Incoraggiare a non aprire link o allegati da mittenti sconosciuti.

7. Comportamento etico online:**

Promuovere il rispetto e l'etica digitale, insegnando a trattare gli altri online con la stessa considerazione che si desidera ricevere.

8. Uso responsabile dei dispositivi:**

Imparare a utilizzare in modo responsabile computer, tablet e smartphone, regolando il tempo trascorso online e bilanciando l'uso dei dispositivi con altre attività.

9. Segnalazione di situazioni sospette:**

Incoraggiare gli studenti a parlare con un adulto di fiducia se si imbattono in contenuti inappropriati o situazioni online sospette.

10. Obbligo di Aggiornare il Software:

Insegnare a mantenere costantemente aggiornato il sistema operativo e tutti i programmi installati per beneficiare delle ultime patch di sicurezza.

11. Pericolo Sito non HTTPS:

Spiegare come evitare di inserire informazioni personali su siti web non sicuri o senza connessione HTTPS per prevenire il rischio di furto di dati.

12. Divieto di Download di Materiali Sospetti:**

Informare sui pericoli di scaricare o aprire file provenienti da fonti non attendibili o sospette al fine di evitare malware e minacce informatiche.

14. Pericolo Comunicazioni Sospette:**

Responsabilizzarli a segnalare immediatamente qualsiasi comunicazione sospetta o messaggio da parte di sconosciuti e a non condividere informazioni personali online.

15. Obbligo di Utilizzare la VPN su WiFi Pubblici:**

Insegnare alla connessione sicura su reti WiFi pubbliche, con obbligo di utilizzare una VPN per garantire una connessione sicura e proteggere i dati personali da potenziali attacchi.

16. Divieto di Partecipazione ad Attività Malevole:**

Responsabilizzare sugli illeciti: divieti a partecipare o contribuire ad attività online illegali o dannose, come hacking, phishing o diffusione di malware.

17. Divieto di Condivisione delle Password:**

Responsabilizzarli alla non condivisione delle proprie password con nessuno, nemmeno con amici. Le password sono personali e la loro condivisione può compromettere la sicurezza dell'account.

18. Collaborazione con i genitori:**

Coinvolgere i genitori nel processo educativo sulla sicurezza cibernetica, fornendo loro strumenti per monitorare e gestire l'attività online dei loro figli. La sicurezza cibernetica è un processo educativo continuo e collaborativo che coinvolge insegnanti, genitori e studenti.

INDICAZIONI PER I GENITORI

Il Garante per l'Infanzia ha recentemente fornito indicazioni chiare in merito alle soglie minime per l'apertura di un account e la conclusione di un contratto per servizi su Internet. Secondo il Garante, il consenso al trattamento dei dati personali può essere autonomamente fornito solo da coloro che hanno compiuto 14 anni; prima di questa età, è necessario ottenere l'assenso dei genitori. La legge italiana specifica che la soglia minima per concedere il consenso "privacy" è di 14 anni, come stabilito nell'articolo 2-quinquies del codice della privacy.

Quando si firma un contratto, ad esempio, per l'adesione a un social network, è importante rispettare il limite di 18 anni fissato dalla legge italiana per la capacità di concludere un contratto valido. In altre parole, il consenso al trattamento dei dati personali può essere fornito autonomamente solo da chi ha compiuto 14 anni, mentre per stipulare un contratto con un fornitore di servizi digitali è necessaria la maggiore età, acquisita a 18 anni.

È auspicabile che l'utilizzo dei dati a fini di marketing non sia generalmente consentito e, qualora lo sia, che sia rispettoso della condizione di minore età e del grado di maturità. Inoltre, è necessario evitare la profilazione del minorenne, a meno che non sia per scopi di tutela e sicurezza.
In pratica, in base al codice civile italiano, un bambino non può concedere il consenso privacy né stipulare un contratto valido, soprattutto uno che possa comportare rischi per il suo benessere, come nel caso di un contratto con un social network. La stessa considerazione si applica al consenso per finalità di marketing, senza limiti di età.

CONSIGLI PER LA SICUREZZA CYBERNETICA DEI PROPRI FIGLI. COINVOLGIMENTO ATTIVO DEI GENITORI

- **Promuovi attività all'aperto:**

Se noti che il tuo bambino/a o ragazzo/a trascorre troppo tempo online, suggerisci attività all'aperto o qualcosa che solitamente vi piace fare insieme. Questo aiuta a distogliere l'attenzione dagli schermi e a promuovere un sano equilibrio tra attività virtuali e fisiche.

- **Vigila costantemente sui contatti Online:**

Monitora in modo attivo i contatti online e le app di gioco del tuo bambino/a o ragazzo/a. A questa età, possono essere facilmente influenzati, spaventati o manipolati. Mantieni un dialogo aperto e incoraggia tuo figlio/a a condividere eventuali preoccupazioni.

- **Stabilisci regole chiare sul tempo Online:**

Definite insieme delle regole chiare sul tempo da trascorrere online. Questo chiarisce che, se l'accesso è limitato, ci sono anche rischi associati. Coinvolgi tuo figlio/a nella definizione di queste regole, in modo che le comprenda e le rispetti.

- **Insegnagli la diffidenza Online:**

Anche se sembra ancora molto piccolo/a, parla del concetto che online non si sa mai chi si cela dietro uno schermo. Spiega l'importanza di essere diffidenti e di chiedere ai genitori o agli adulti di fiducia se qualcuno sconosciuto tenta di contattarli.

- **Attiva Parental Control e mantieni la password riservata:**

Imposta un sistema di parental control per limitare l'accesso a contenuti inappropriati. Tieni la password segreta e aggiornala regolarmente. Questo garantisce un controllo efficace sull'uso dei dispositivi.

- **Risorse per i Genitori:**

Familiarizza con risorse specifiche per i genitori sulla sicurezza online, compresi consigli per affrontare il cyberbullismo, indicazioni sulla navigazione sicura per diverse fasce d'età e consigli sull'uso sicuro del telefono cellulare per i bambini.

- **Domanda e Supporto:**

Invita tuo figlio/a a condividere eventuali dubbi o preoccupazioni sulla sicurezza online. Stabilisci una comunicazione aperta in modo che si senta a suo agio nel parlare dei suoi incontri online. Promuovendo una partecipazione attiva e consapevole dei genitori nella vita digitale dei loro figli, si crea un ambiente in cui la sicurezza online diventa una priorità condivisa.

CONSIGLI PER I GENITORI IN MERITO AI RISCHI ONLINE CHE COINVOLGONO I MINORI

- **Adescamento online:**

Informa i tuoi figli sul pericolo dell'adescamento online. Sottolinea che non devono mai condividere informazioni personali o immagini con estranei online. Incoraggiali a parlarti se avvertono comportamenti sospetti e assicurati che siano consapevoli che le persone online potrebbero non essere chi dicono di essere.

- **Cyberbullismo:**

Parla con i tuoi figli dell'importanza del rispetto online. Sottolinea che le azioni online, anche quelle apparentemente innocenti, possono avere conseguenze dolorose per gli altri. Promuovi la consapevolezza del cyberbullismo e incoraggiali a rispettare la privacy degli altri e a essere cauti nelle interazioni online.

- **Diffusione e detenzione di materiale illegale:**

Spiega ai tuoi figli i rischi legati alla diffusione e alla detenzione di materiale illegale online. Sottolinea che partecipare a gruppi di messaggistica o condividere immagini illegali costituisce un reato. Incoraggiali a segnalare immediatamente qualsiasi contenuto sospetto a commissariatodips.it o alle autorità competenti.

- **Challenge online:**

Discuti con i tuoi figli sulle sfide online e sulla loro potenziale pericolosità. Mettili in guardia sul fatto che alcune sfide potrebbero comportare rischi reali e che la popolarità online non dovrebbe mai mettere a repentaglio la loro sicurezza. Promuovi un atteggiamento critico verso le tendenze online e incoraggiali a valutare attentamente i rischi prima di partecipare a qualsiasi sfida.

In generale, è fondamentale mantenere una comunicazione aperta e onesta con i tuoi figli riguardo alla loro attività online. Fornisci loro le conoscenze necessarie per navigare in modo sicuro nel mondo digitale e sii disponibile per affrontare qualsiasi preoccupazione o domanda che possano avere.

CONSIGLI PER I GENITORI FINALIZZATI A GARANTIRE UN USO SICURO DI INTERNET DA PARTE DEI LORO FIGLI

- **Posizionate il computer in una stanza frequentata da tutti:**

Tenete il computer in una zona della casa frequentata da tutti i membri della famiglia. Questo favorirà una maggiore trasparenza sulle attività online e permetterà un controllo più agevole.

- **Controllate regolarmente le attività online:**

Effettuate regolarmente controlli sulle attività online del vostro figlio. Questo vi permetterà di monitorare il tipo di contenuti a cui accede e di intervenire tempestivamente in caso di situazioni rischiose.

- **Dialogate sulle attività online gradite:**

Parlate con vostro figlio del tipo di attività online che gli interessano. Conoscere i suoi interessi online vi aiuterà a capire meglio il suo mondo digitale e a fornire consigli mirati.

- **Esaminate file, cronologia e attività online:**

Comunicate chiaramente a vostro figlio che periodicamente esaminerete i file del computer, la cronologia del browser e le sue attività online. Questo contribuirà a promuovere la responsabilità nell'uso del dispositivo.

- **Verificate profili e messaggi online:**

Cerca online il nome di vostro figlio, esaminando i suoi profili e i messaggi postati sui siti frequentati dai teenager. Analizzate le pagine web o i blog che visita per garantire un ambiente online sicuro.

- **Comunicate la possibilità di rivedere attività online private:**

Informate vostro figlio che potreste rivedere le sue attività di comunicazione privata online se avete motivo di pensare che si stia comportando in modo poco prudente o responsabile.

- **Siate vigili su comportamenti sospetti:**

State attenti a comportamenti che sembrano nascondere qualcosa, come il rapido cambio di schermata quando vi avvicinate al computer o tentativi di eliminare le tracce della navigazione online.

- **Insegnate regole base per un uso sicuro di Internet:**

È importante insegnare ai vostri figli alcune regole di base per un uso sicuro di Internet. Queste possono includere l'importanza della privacy online, il riconoscimento di situazioni rischiose e

l'adozione di comportamenti responsabili. Seguire questi consigli contribuirà a creare un ambiente online sicuro per i vostri figli e promuoverà un uso responsabile della tecnologia.

CONSIGLI PER GLI STUDENTI RIGUARDO ALLA GESTIONE DI SITUAZIONI MOLESTE ONLINE

- **Non rispondere a E-mail o SMS molesti ed offensivi:**

Evita di rispondere a messaggi e SMS che sono molesti o offensivi. Ignorare tali comunicazioni può spesso essere la risposta migliore.

- **Non rispondere a chi ti insulta o prende in giro:**

Non cadere nella trappola di rispondere agli insulti o alle prese in giro online. Mantieni un comportamento rispettoso e distanziato.

- **Non rispondere a chi ti offende in Chat o ti "butta fuori" dalla Chat Room:**

Se qualcuno ti offende o ti caccia da una chat room, evita di reagire in modo negativo. Abbandona la stanza e segui le procedure di sicurezza.

- **Salva i messaggi offensivi che ricevi (SMS, MMS, E-mail):**

Conserva i messaggi offensivi che ricevi come prova. Possono essere utili se si decide di segnalare l'incidente alle autorità.

- **Prendi nota del giorno e dell'ora in cui il messaggio ti è stato inviato:**

Annota con precisione il momento in cui ricevi messaggi offensivi. Queste informazioni possono essere cruciali se è necessario intraprendere azioni legali.

- **Cambia il tuo nickname:**

Se stai vivendo molestie online, considera la possibilità di cambiare il tuo nickname per mantenere un profilo più discreto.
Cambia il numero del tuo telefonino e comunicalo solo a pochi e fidati amici.
Nel caso di molestie tramite telefono, cambia il numero e condividilo solo con persone di tua fiducia.

- **Usa i filtri per bloccare le E-mail moleste:**

Sfrutta i filtri di sicurezza disponibili sulle tue piattaforme di comunicazione per bloccare messaggi indesiderati.

- **Non fornire mai dati personali (nome, cognome, indirizzo di residenza, etc):**

Mantieni la tua privacy online. Non fornire mai dati personali a persone sconosciute.
Se qualcuno in CHAT ti chiede di incontrarti, rispondi "NO, GRAZIE!":

- **Se ricevi richieste sospette, rifiutale prontamente.**

Non accettare incontri con persone conosciute solo online.
Parlane immediatamente con un adulto (genitori e/o docenti).In caso di molestie online, condividi immediatamente l'esperienza con un adulto di fiducia, come genitori o insegnanti.

- **Nel caso di minacce fisiche o sessuali, contatta la POLIZIA:**

Se le molestie online raggiungono il livello di minacce fisiche o sessuali, contatta immediatamente le autorità competenti, come la polizia.

Questi consigli mirano a garantire che gli studenti possano navigare in modo sicuro e responsabile nel mondo online, proteggendo la propria privacy e reagendo prontamente a situazioni potenzialmente pericolose.

Minacce Digitali: Esplorando i Reati sulla Cybersicurezza nel Mondo Virtuale.

- **Flaming:**

Consiste nella pubblicazione di messaggi dal contenuto aggressivo, violento, volgare, denigratorio, in danno di un utente nel momento in cui questi compie una determinata attività online (ad esempio quando esprime il suo pensiero intervenendo su un social network);

- **Harassment**:

consiste nell'invio continuo e reiterato di una moltitudine di messaggi informatici di carattere volgare, aggressivo e minatorio (attraverso strumenti di comunicazione come sms, e-mail, chat, social network, ecc...) da parte di uno o più soggetti nei confronti un individuo assunto come bersaglio

- **Denigration:**

consiste nella diffusione in via informatica o telematica di notizie, fotografie o video (veri o anche artefatti riguardanti comportamenti o situazioni imbarazzanti che coinvolgono la vittima), con lo scopo di lederne l'immagine, offenderne la reputazione o violarne comunque la riservatezza.

- **Impersonation:**

consiste nelle attività non autorizzate poste in essere da un soggetto il quale, dopo essersi in qualche modo procurato le credenziali di accesso ad uno o più account di servizi online in uso alla vittima, se ne serve per creare nocumento o imbarazzo (ad esempio attraverso l'invio di messaggi o la pubblicazione di contenuti inopportuni, facendo credere che gli stessi provengano dalla vittima)

- **Outing and trickery:**

consiste nella condotta di chi, avendo ricevuto o detenendo dati, immagini intime o altro materiale sensibile della vittima (ricevuti direttamente da quest'ultima o, comunque, realizzati con il suo consenso), li diffonde tramite messaggi, chat o social network o comunque li carica in rete senza l'approvazione della vittima o addirittura contro la sua esplicita volontà, rendendoli così accessibili ad una moltitudine di utenti.

- **Cyberstalking:**

consiste nell'invio ripetuto di messaggi che includono esplicite minacce fisiche, al punto che la vittima arriva a temere per la propria incolumità.

- **Sexting**:

consiste nell'invio di messaggi via smartphone e internet, corredati da immagini a sfondo sessuale.

- **Exclusion:**

escludere intenzionalmente da un gruppo online, da una chat, da un game interattivo o da altri ambienti protetti da password "bannare".
L'EXCLUSION è una severa punizione, riduce i contatti, la popolarità e il potere.