Guida per un uso sicuro e responsabile della rete



ISTITUTO COMPRENSIVO
PIAZZA FILATTIERA 84

Lo scopo delle presenti linee guida, elaborate nel formato di rapida consultazione dell'infografica, è, da un lato, fornire a genitori e alunni dell'Istituto un'iniziale consapevolezza di quali siano **le criticità della navigazione su internet** e dell'uso di strumenti e device digitali; e, dall'altro, **condividere le buone pratiche per garantire una fruizione efficiente e sicura della rete**, o quantomeno ridurre l'esposizione ai rischi inerenti alla tecnologia.

Nonostante la complessità crescente dei sistemi online, che possono lasciare confusi, è infatti importante che il *navigante*, che sia giovane o meno, abbia una prima formazione almeno rispetto ad alcuni ambiti chiave, quali **la sicurezza informatica** (per evitare intrusioni e altri spiacevoli incidenti); **la privacy personale** (perché tutta l'attività online lascia un'impronta difficile da cancellare); **le modalità di interazione con gli altri utenti** (affinché gli ambienti digitali in cui conviviamo siano accoglienti e improntati al reciproco rispetto); **le caratteristiche delle Intelligenze Artificiali** (le cui grandissime potenzialità non devono mai metterne in ombra limiti e lati oscuri); **la capacità di orientarsi nelle informazioni disponibili**, spesso incomplete, errate o persino deliberatamente false (*fake news*), e nella cui enorme mole l'utente rischia di perdere l'orientamento (fenomeno che gli esperti chiamano *infodemia*).

Infine, abbiamo incluso **una piccola guida all'account Google Workspace** che il nostro IC offre ad alunni e docenti in supporto alle attività didattiche.

Mettiamo, quindi, questo documento a disposizione di tutta la comunità scolastica, nella consapevolezza che un certo grado di competenza nell'uso dei servizi informatici non solo è essenziale per tutti noi (visto che ne fruiamo quotidianamente), ma **sarà fonramentale per i cittadini di un domani in cui lo scambio di messaggi e informazioni in rete avrà un ruolo ancora più importante.**



Il Team Digitale dell'IC Piazza Filattiera 84

Cos'è l'Identità Digitale?

IDENTITÀ PERSONALE VS DIGITALE



Realtà tangibile e privata



Insieme delle nostre attività in rete: messaggi, foto, interessi, shopping, luoghi visitati, amicizie sui social...



Per i ragazzi di oggi, le due identità si sviluppano di pari passo.



TRACCIA INDELEBILE

Le tracce della nostra attività online possono restare online potenzialmente per sempre, contribuendo alla nostra reputazione. Potrebbero finire in mano a un datore di lavoro. Siamo responsabili per i nostri dati, come per quelli degli altri (ad es., condividendo foto che ritraggono altre persone).

Gli adolescenti tendono a condividere online moltissimi dettagli delle loro vite (*Oversharing*). Questo può avere in futuro ripercussion inattese sulla loro reputazione



VALUTA PRIMA DI CONDIVIDERE!



Attenzione a informazioni come geolocalizzazione, foto e indirizzo di casa...
Evita di taggare o pubblicare immagini di altre persone **senza il loro esplicito consenso**



DATI AD ALTO RISCHIO

Informazioni da non condividere mai con leggerezza, perché possono portare a rischi per la privacy con conseguenze anche gravi:



Video, foto, indirizzi, nomi e cognomi



Codice fiscale, dati bancari, numeri di carte di pagamento



Opinioni politiche, convinzioni religiose, dati giudiziari





SICUREZZA INFORMATICA

Usa login sicuro (autenticazione a due fattori, passkey...) per i servizi importanti che hanno accesso ai tuoi dati personali.
Diffondere password e codici di sblocco **espone non solo a scherzi o a cyberbullismo, ma anche a hacking e frodi.**



ETÀ DEL CONSENSO DIGITALE

I minori di 14 anni non possono dare il consenso al trattamento dei propri dati personali, richiesti da molti servizi online. E' necessario il permesso di chi esercita la responsabilità genitoriale.
Molti social prevedono il limite di età di 16 anni per l'iscrizione.

ISTITUTO COMPRENSIVO PIAZZA FILATTIERA 84

Cyber-sicurezza in rete

Bastano alcuni semplici accorgimenti per evitare danni, manomissioni o furto di dati dai nostri device.
Se però subiamo lo stesso un attacco informatico, la Polizia Postale può intervenire in nostro aiuto.

TECNOLOGIE

AUTENTICAZIONE A DUE FATTORI



Attiva un secondo codice di sblocco o dati biometrici per proteggere social, mail e videogiochi. **Così impedisci a un hacker di entrare** anche se conosce la password.

GLI AGGIORNAMENTI CI PROTEGGONO

Installa sempre gli aggiornamenti: correggono le vulnerabilità software di recente scoperta. Gli hacker hanno bisogno di una falla di sicurezza per prendere controllo di un sistema; **i device non aggiornati sono facilmente attaccabili.**



IN PUBBLICA PIAZZA

Le reti Wi-Fi pubbliche sono a rischio cattura di dati e **non dovrebbero essere usate per servizi sensibili.**



BUONE PRASSI

LA PASSWORD E'... UNO SPAZZOLINO

E' personale e non va condivisa.
Non usare la stessa per tutti i siti.



MEGLIO "P455wORd_" o "p@Ssw0rD"?



Le regole per le password possono sembrare assurde, ma servono alla nostra protezione. Un Password Manager può memorizzarle al posto nostro, garantendo comodità e un ottimo livello di sicurezza.
Le più importanti andrebbero cambiate di tanto in tanto, evitando nomi, date, e parole o sequenze comuni.

PRIMA DI CLICCARE... PENSA



Cliccare su di un link maligno può esporre a ***phishing***, o, nei casi più gravi, addirittura compromettere il device.
Attenzione anche a giochi e App sospette: possono essere dei *cavalli di Troia* in grado di infettare il dispositivo.





***PHISHING**: copie di siti legittimi, messe in piedi da hacker per convincere un utente a inserire le credenziali di accesso e così rubarle*

IL RUOLO DEGLI ADULTI

UNA VERA BARRIERA

Le funzioni di **parental control** inoltrano ai genitori l'approvazione per l'installazione delle app (consentendo di bloccare quelle "sospette"), permettono di revocare i permessi (come l'accesso ai contatti o alla fotocamera), e segnalano eventuali utilizzi illeciti di un account.
Insomma, costituiscono **una vera barriera contro i cyberattacchi.**

SEGNALAZIONI E DENUNCE

Dal sito della polizia postale si può fare:

- **Segnalazione** se non ci sono vittime (ad es., si scova in rete un sito fraudolento o con contenuti illegali)
- **Denuncia** (in caso si sia vittime di cyberbullismo, condivisione di materiale privato, hacking...)



IL DIALOGO E' LO SCUDO MIGLIORE

Un clima di fiducia in famiglia è essenziale; in caso di cyberattacco, la paura di una punizione come il sequestro del telefono può portare a nascondere l'evento, rallentando le azioni necessarie per affrontare l'emergenza.



Social Media sicuri per Genitori e Adolescenti

I RAGAZZI E I SOCIAL

dati: sondaggio dell'Associazione Nazionale Presidi e eTutorweb "Osservare Oltre"



84%

Possiede un profilo social e usa il cellulare quotidianamente.



87%

Considera l'approvazione digitale fondamentale per la propria immagine.



91%

Non comunica ai genitori le proprie attività online.



Rispetto di etica e netiquette
Chiedere il consenso prima di taggare gli altri; non pubblicare contenuti compromettenti o che possono mettere in imbarazzo.
Niente comportamenti verbalmente aggressivi: ci si deve relazionare online come di persona, rispettando la sensibilità altrui.

IDEE CHIAVE

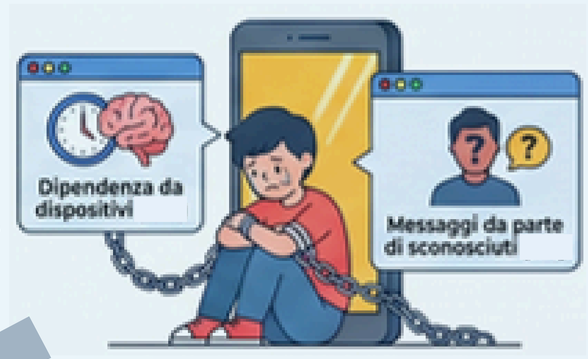
Requisiti di accesso
I profili social devono essere creati solo al raggiungimento dell'età minima prevista dalla legge, utilizzando la funzione "profilo teen" ove disponibile.





Navigare a vista
I social (e internet in generale) mettono in contatto con un'incredibile varietà di idee, persone, contenuti e situazioni. Ciò può lasciare i giovani naviganti confusi, disorientati, causare ansia o persino traumi. Gli adulti devono essere pronti ad assistere i ragazzi in caso di esperienze negative.

RIDURRE L'ESPOSIZIONE AI RISCHI



Il Contratto Genitori-Figli
Creare un accordo, anche scritto, per definire le regole di uso dei social.



Limiti di tempo e spazio
Utilizzare i dispositivi solo in orari prestabiliti e negli spazi comuni della casa.





Segnali di allarme: ritiro sociale, irritabilità, perdita di interesse per altre attività.



Protezione dei dati e Privacy
Impostare la massima privacy. Non condividere indirizzi o numeri di telefono. Abilitare login sicuro (es. autenticazione a due fattori).



Incontri e contatti reali
Interagire solo con persone conosciute dal vivo; evitare incontri con persone del mondo online, se non con la supervisione dei genitori



Identità... social
Utilizzare nickname o varianti del nome reale può proteggere da interazioni sgradite.

Cyberbullismo: conoscerlo, riconoscerlo, difendersi

Il cyberbullismo è l'uso inappropriato della rete per scambiare contenuti violenti e discriminatori ai danni di coetanei.
Bambini e adolescenti sono i primi che, con il loro comportamento, possono evitare situazione spiacevoli on line.
E' importante conoscere quali sono le tattiche dei bulli, le conseguenze legali e i passi fondamentali che studenti e adulti possono intraprendere per fermare l'abuso..

LE MODALITA' DEL CYBERBULLO

MOLESTIE VIA CHAT: messaggi privati ripetuti, offensivi e/o denigranti, che possono sfociare nella minaccia.





FURTO DI IDENTITA' e INGANNO: i cyberbulli possono spacciarsi per altre persone, per la vittima, riuscire a ottenere le credenziali per accedere ad un social e pubblicare contenuto diffamatorio o ottenere informazioni private.

FLAMING: stile comunicativo violento e volgare, fuori tema, col solo scopo di ferire.



ESCLUSIONE SOCIALE: emarginazione della vittima da un gruppo online.



PUBBLICAZIONE DI MATERIALE, anche privato, imbarazzante o che mette in cattiva luce la vittima.



PREVENZIONE E DIFESA







1) **Non rispondere agli insulti**, non contribuire a far circolare materiale offensivo contro altri
2) **Salva le prove** (screenshot con data e ora)
3) **Blocca i contatti molest**i, cambia password e numeri di telefono, usa impostazioni di privacy, non navigare nei siti dove sei stato attaccato.





Per gli adulti: monitorare i cambiamenti di stato d'animo, salute, ansia, mancanza di denaro. In caso di episodi verificatisi, attivare reti di supporto con la scuola e altri adulti di riferimento, e coinvolgere le Forze dell'Ordine.



In caso di contatti molesti subiti online, cercare il supporto di un adulto è essenziale. Non provare alcun tipo di vergogna: non sei tu ad esserti comportato male.



I service provider sono tenuti ad oscurare e rimuovere contenuti abusivi entro 48 ore dalla segnalazione.

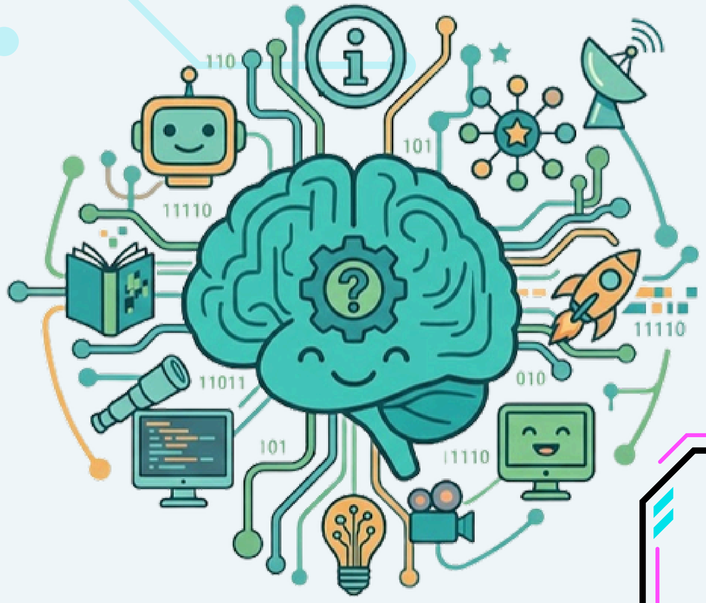


I reati ai quali va incontro un cyberbullo possono essere: diffamazione, minaccia, trattamento illecito di dati personali, violazione privata, estorsione, detenzione di materiale pedopornografico. N.B. ogni volta che si usa il telefonino o si naviga on line si lasciano impronte che possono essere sempre rintracciate dalle Forze dell'Ordine.

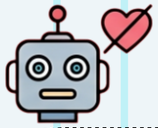
ISTITUTO COMPRENSIVO
PIAZZA FILATTIERA 84

Guida pratica all'uso dell'Intelligenza Artificiale

L'intelligenza artificiale si trova ormai ovunque: sui social, sui siti web e integrata nelle app del nostro telefono. Conosciamola per usarla meglio, senza esserne usati.



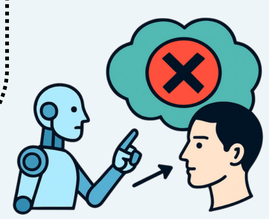
LIMITI DELL'IA



IL ROBOT NON HA EMOZIONI

L'IA **non è adatta a fornire consulenza emotiva o relazionale.** Si sono verificati incidenti in cui **chatbot hanno spinto a comportamenti gravi e autolesivi.**

BIAS E PREGIUDIZIO



Nella fase di *training*, **l'IA assorbe luoghi comuni e pregiudizi;** inoltre, **tende a compiacere l'utente e dargli ragione.**
Per lo sviluppo del senso critico e per la propria crescita personale bisogna integrare sempre le sue informazioni con punti di vista diversi.

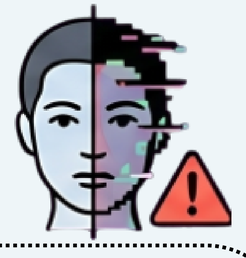
LE ALLUCINAZIONI



L'IA può inventare fatti o dati con estrema sicurezza; verifica sempre su fonti diverse.

REGOLE PER UN USO CONSAPEVOLE

OCCHIO AI DEEPFAKE



I modelli IA permettono di **generare audio e video di qualsiasi persona**, e non è sempre facile capire che si tratta di un falso. **Diffida di ciò che appare strano.**

TIENI ACCESO IL CERVELLO!



Usa l'IA per spunti critici, ma **non lasciare che sostituisca il tuo studio.**
Farsi fare i compiti da un bot è moralmente discutibile, oltre che inutile.

LA TUA PRIVACY E' PREZIOSA



Non condividere mai dati sensibili: **tutto ciò che scrivi a un chatbot viene memorizzato.**

ISTITUTO COMPRENSIVO PIAZZA FILATTIERA 84

Fake News: Guida alla Sopravvivenza Digitale

Anatomia di una Fake News

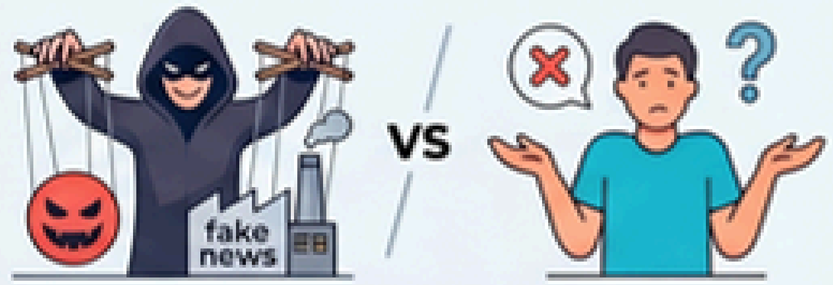


L'esca emotiva e i pregiudizi
Sfruttano rabbia e paura per spingerci a condividere impulsivamente contenuti che confermano le nostre idee.

I segnali di allarme visivi
Diffida di titoli urlati, URL sospetti, errori grammaticali, linguaggio che non lascia spazio alle incertezze, immagini che appaiono ritoccate.



Disinformazione vs Inaccuratezza
Alcune notizie sono create per manipolare, altre nascono semplicemente da una mancata verifica dei fatti.



Le fake news sono informazioni ingannevoli progettate per sfruttare le nostre emozioni e pregiudizi. La difesa principale è la vigilanza: imparare a identificare i segnali di allarme e verificare sistematicamente le fonti per interrompere la catena della disinformazione.

La Checklist del Detective Digitale





Verifica Fonte, Autore e Data
Controlla la sezione "Chi siamo" dei siti da cui prendi informazioni, cerca informazioni su affiliazioni o conflitto d'interessi dell'autore, assicurati che la notizia sia attuale.



Confronta le testate
Una notizia attendibile è solitamente riportata da più agenzie stampa professionali e indipendenti.

Esci dalla "Camera dell'Eco"
Considera i tuoi pregiudizi e consulta punti di vista diversi per trarre conclusioni corrette. Esercita il pensiero critico.



Strumenti e siti consigliati per il fact-checking

	Google Immagini/ TinEye	Verificare l'origine e autenticità delle foto
	Bufale.net Butac.it Cicap	Fact Checking e debunking in lingua italiana
	Snopes Polifact	Verifica di notizie e dichiarazioni internazionali



E se mi accorgo di aver condiviso una bufala?
Elimina il post e pubblica una breve rettifica. La trasparenza è fondamentale per mantenere la propria credibilità personale!

ISTITUTO COMPRENSIVO PIAZZA FILATTIERA 84

L'Account istituzionale di scuola

Cos'è

E' un account che appartiene alla scuola, la quale **lo "presta" agli studenti.** Permette l'accesso ad una selezione di app e servizi informatici per la didattica. **È un ambiente protetto:** le funzioni commerciali sono disattivate e l'uso è monitorato da docenti e amministratori. Può essere utilizzato da qualsiasi device, e tutti i dati (file, mail...) **restano accessibili in cloud da qualsiasi luogo ci si connetta**

Attivazione

I coordinatori delle classi prime si occupano, a inizio anno, di comunicare alle famiglie le credenziali e la procedura di accesso.

Buone pratiche

- Gli alunni sono tenuti ad avere sempre le **credenziali a disposizione** (memorizzate, o scritte sul diario o un quaderno), per poter fare login sui device della scuola se la didattica lo richiede
- Account e servizi online di scuola **sono estensioni digitali degli ambienti e dei materiali scolastici** e quindi richiedono lo stesso atteggiamento di rispetto. **Eventuali usi scorretti sono sanzionati**
- In caso di necessità o assistenza (compreso il cambio della password) bisogna rivolgersi all'indirizzo: **team.digitale@filattiera84.edu.it**
- L'Account istituzionale va usato SOLO per i servizi di scuola e didattici. Non è consentito l'utilizzo per iscriversi a videogiochi, social e siti non inerenti alla didattica!

Drive

Spazio di archiviazione
E' una cartella in cloud, cioè non presente fisicamente sul dispositivo. Permette di salvare file e documenti, e accedervi da qualsiasi device (una volta fatto l'accesso con l'account di scuola). Rappresenta un'alternativa più pratica e sicura ai supporti esterni (es., le "chiavette" USB)



Classroom

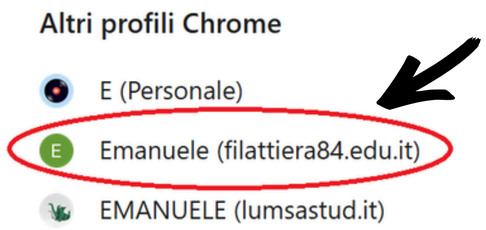
Condivisione di materiali didattici, restituzione all'insegnante lavori e compiti a casa
L'alunno deve essere aggiunto alla classe virtuale dall'insegnante, oppure deve fare login e iscriversi alla classe inserendo un codice specifico (fornito dall'insegnante).

Gmail

Casella di posta elettronica
Qualsiasi comunicazione online con gli insegnanti (ad es. per richiesta di chiarimenti su un compito, ecc) deve passare attraverso posta elettronica, con indirizzo mail istituzionale.

Google Docs, Presentazioni

Editor di testo e di diapositive (slide)
Analoghi di Micorosft Word e Microsoft Powerpoint (e dei programmi equivalenti a questi). Permettono di lavorare in modalità condivisa (contemporaneamente sullo stesso file, anche da remoto). Non è necessario salvare. Tutte le versioni dell'elaborato restano disponibili.



Configurare l'account per l'utilizzo a casa

L'account dovrebbe essere aggiunto ai device personali dell'alunno, ma anche al tablet o computer di uso condiviso a disposizione a casa per le attività didattiche.
Per assicurarsi che ogni familiare abbia accesso solo ai suoi dati di navigazione**, si possono impostare profili separati sia per il device** (ad es., gli utenti di un PC Windows) **che per il browser di navigazione.** In questo modo, dalle opzioni in alto a destra del browser si potrà facilmente passare dai servizi personali (ad es., videogiochi, musica, playlist Youtube private) ai servizi di scuola.

*L'account non contiene dati privati importanti, e deve essere sempre facilmente accessibile dall'alunnno. Perciò, in questo caso specifico, non è sbagliato scegliere una **password semplice**, e evitare di cambiarla (salvo eventi particolari).*