ISTITUTO COMPRENSIVO DI PALMANOVA

# SICUREZZA E BUONE PRATICHE PER NAVIGARE ONLINE

a.s. 2024/2025

Indicazioni per genitori
e alunni

*Cari Genitori,*

*Questo opuscolo vuole essere una sintesi di quanto noi operatori della Scuola, vista la leggerezza con cui i ragazzi utilizzano la tecnologia, sentita la Polizia Postale, vorremmo poter condividere con voi, in termini di sicurezza della navigazione online per i ragazzi che giornalmente ci affidate e di cui abbiamo massima cura e rispetto.*

*Citando le Norme vogliamo ricordarvi quali sono le responsabilità che vi prendete tutte le volte che affidate un dispositivo con collegamento internet ai vostri figli, sia esso un tablet, uno smartphone, un PC, una consolle per videogiochi o anche solo la Smart TV di ultima generazione che avete installato in salotto! Conoscete i rischi a cui sono sottoposti i minori? È nostra preoccupazione far crescere in responsabilità i ragazzi e le ragazze, ma senza il vostro sostegno siamo certi che il nostro lavoro sarebbe vano.*

*Leggete queste indicazioni prima da soli, senza fretta, ma leggetele. Troverete diversi link di approfondimento, pagine selezionate da siti autorevoli come quello del Commissariato di P.S.- Sportello per la sicurezza degli utenti del Web e quello di Generazioni Connesse- Safer Internet Centre, che da anni collaborano con la Scuola per la prevenzione, informazione e formazione del personale e degli studenti.*

*Vi suggeriamo, poi, di condividere in base all'età dei vostri figli o alle esigenze specifiche, una o l'altra sezione qui trattata... e di non smettere mai di vigilare!!*

*Pronti?!*

*Buona lettura*

Il ref. per il Cyberbullismo
*Elena Bernardis*

Il Dirigente Scolastico
*Matteo Tudech*

## INTRODUZIONE

Con l'entrata in vigore della Legge 71/2017 (Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo) la Scuola Italiana è tenuta a mettere in atto azioni preventive, educative e ri-educative rivolte a tutti i minori coinvolti in episodi di cyberbullismo, sia che si trovino nella posizione di vittime sia in quella di responsabili di illeciti, nonché occasioni formative e di confronto con le famiglie.

Secondo i dati in possesso ai Commissariato di pubblica sicurezza, ad oggi le minacce cibernetiche più frequenti in adolescenza sono rappresentate da:

### Adescamento online

Un numero crescente di adulti utilizza la rete e i servizi di socia networking, le app di gioco online per agganciare minorenni allo scopo di farsi mandare immagini erotiche e sessuali, spesso fingendosi coetanei innamorati delle loro vittime.

*(vedi pagina seguente – Fasi dell'adescamento dei minori online)*

### Cyberbullismo

I ragazzi spesso non hanno adeguata consapevolezza i quanto i "dispetti" online, le prese in giro possano avere effetti dolorosi sugli altri. Parlate del rispetto della privacy anche online, della necessità di essere riservati con le proprie immagini e quelle degli altri per aiutarli ad evitare di ritrovarsi bulli senza l'intenzione di fare del male.

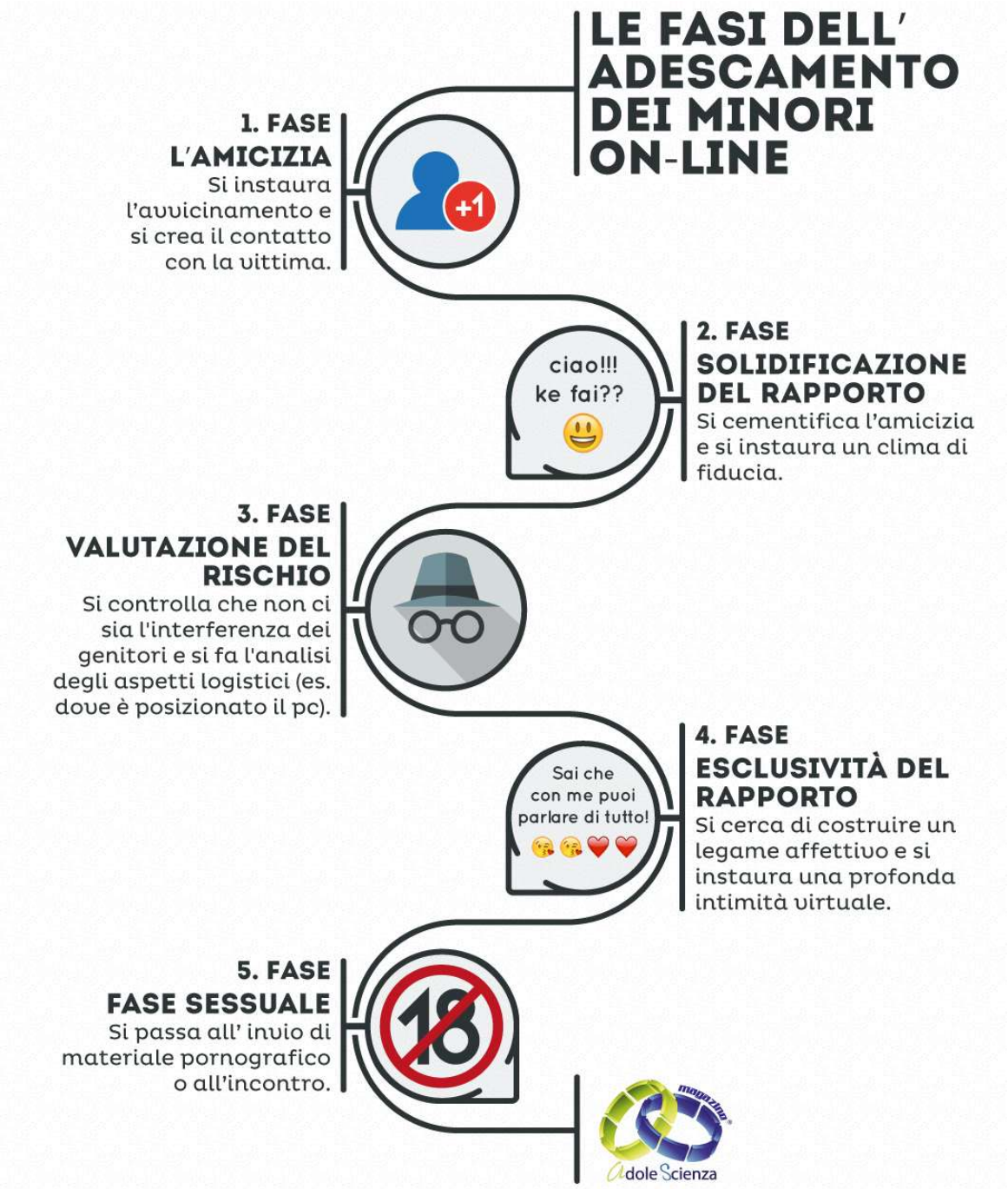
### Diffusione e detenzione di materiale illegale

I ragazzi vengono continuamente aggiunti in gruppi di messaggistica istantanea da altri coetanei, conoscenti e amici. Non sempre prestano le dovute attenzioni alla natura di questi gruppi e alle foto e filmati che ci si scambia. È fondamentale che siano consapevoli che chiunque contribuisca a diffondere immagini sessuali e di violenza che riguardino bambini e ragazzi minorenni commette un reato: è utile invece segnalare subito al Commissariato di P.S. la presenza di questo tipo di materiale su chat e siti online.

### Challenge online

È un fenomeno molto diffuso tra i ragazzi che consiste nel filmarsi mentre si fanno azioni che in quel momento sono trend topic su socialnetwork e circuiti da loro frequentati. Nella maggioranza dei casi si tratta di azioni poco pericolose ma occorre sensibilizzare i ragazzi sul fatto che alcune sfide possono comunque rappresentare un pericolo se intraprese con l'obiettivo di aumentare la propria popolarità, senza valutare i rischi reali.

**Sezione Operativa per la Sicurezza cibernetica (S.O.S.C.)**
**Udine – Via L. Uccellis n. 4**
**tel. 0432 223248**




***Per approfondire:***

- Adescamento online
- Pedofilia online
- Grooming
- Pedopornografia online

## UTILIZZO DEI DISPOSITIVI: TEMPI E MODI… E SE FOSSI DIPENDENTE?

### Fai il test

| Domanda | SI | NO |
|---|---|---|
| Non riesci a staccarti dal pc o dallo smartphone e stai online fino a tarda notte? | ☐ | ☐ |
| Nessun'altra attività ti dà soddisfazione come essere online, ad esempio, per chattare o giocare? | ☐ | ☐ |
| Esci sempre meno e trascorri sempre meno tempo con i tuoi amici, pur di stare online? | ☐ | ☐ |
| Comunichi sempre meno con la tua famiglia, perché preferisci stare on-line? | ☐ | ☐ |
| Guardi l'orologio e ti accorgi di aver trascorso ore online senza che tu te ne accorgessi? | ☐ | ☐ |

Se hai risposto sì anche solo ad una di queste domande, *forse*, dovresti ripensare un po' al tuo rapporto con le tecnologie e con la Rete.

***Per approfondire:***

- Dipendenza online
- Effetti dell'uso prolungato dei dispositivi sui bambini/ragazzi
- Dipendenza da videogiochi

### Fascino e potere dei Social: conoscere e usare al meglio le App di Messaggistica

Clicca sul logo per saperne di più:





## REPUTAZIONE ONLINE

https://www.generazioniconnesse.it/site/it/2022/02/25/chi-sono-online/

### Quando siamo online, cosa dovremmo evitare per non danneggiare la nostra web-reputation?

- Non dimentichiamo di filtrare i contenuti: **ciò che pubblichiamo online resta**. Quindi, evitiamo di pubblicare contenuti inopportuni e potenzialmente compromettenti per la nostra immagine.
- Usiamo le impostazioni sulla privacy. È importante fare in modo che solo i nostri amici abbiano accesso ai contenuti che pubblichiamo, soprattutto quelli più privati.
- Cerchiamo di non postare contenuti che criticano gli altri.
- Non usiamo un linguaggio volgare, scurrile e scorretto da un punto di vista linguistico.
- Non condividiamo contenuti falsi o di cui non abbiamo la certezza.

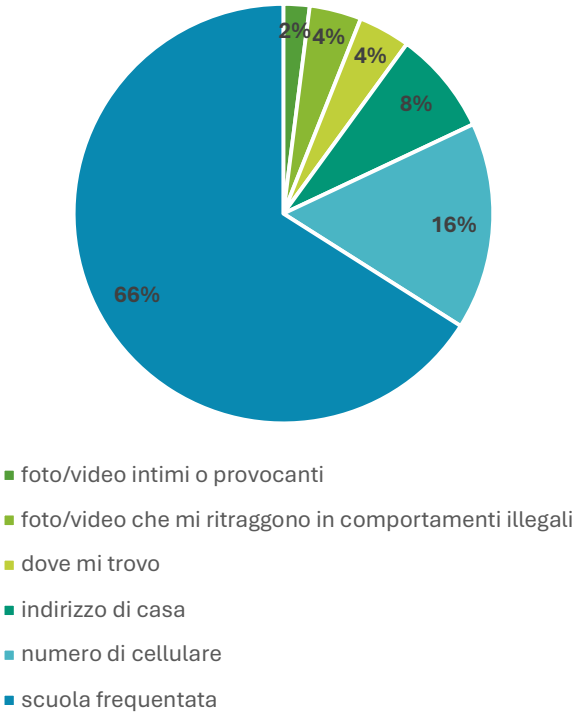
### E quando altri danneggiano la nostra reputazione si chiama body-shaming, che fare?

https://www.generazioniconnesse.it/site/it/2022/02/25/il-body-shaming/

### E quando i genitori postano contenuti relativi ai propri figli... si chiama sharenting

https://www.generazioniconnesse.it/site/it/2020/02/18/lo-sharenting/

### Se qualcuno mi cerca online, trova...




Solo 1 persona su 3 non lascia queste informazioni online.

***Per approfondire:***

- Privacy

**Internet è pubblico e non dimentica!**

## RESPONSABILITÀ DEI MINORI: COSA DICE LA LEGGE?

Il sistema penale minorile italiano si costruisce intorno al concetto di imputabilità: per poter procedere penalmente nei confronti di un minore è necessario che questi sia imputabile, ovvero che sia stata valutata la capacità del minore per essere dichiarato responsabile di un reato ed essere sottoposto a una pena.

### Principio di imputabilità

L'art. 97 del Codice penale indica che il minore infraquattordicenne non è mai imputabile.

L'art. 98 del Codice penale indica che "è imputabile chi, nel momento in cui ha commesso il fatto, aveva compiuto 14 anni ma non ancora i 18, se aveva capacità di intendere e di volere".

Quindi, ai sensi dell'art. 98 del c.p., per i minori dai 14 ai 17 anni la capacità di intendere e di volere in relazione al reato compiuto deve essere sempre accertata, mentre per gli adulti autori di reato è presunta.

### In sintesi

Per la legge Italiana un ragazzo al compimento dei 14 anni diventa capace di intendere e volere; dunque, è anche in grado di capire le conseguenze delle sue azioni e si assumersi le responsabilità del suo agire.

Se commette reato dopo il 14° compleanno può finire in carcere per ordinanza del Tribunale per i Minorenni. I genitori (e il ragazzo) subiscono dei controlli regolari (Assistenti Sociali – psicologi – educatori) e in caso di denunce la famiglia del minore è tenuta al risarcimento del danno compiuto dal figlio.

## INDIRIZZO IP: LA NOSTRA IDENTITÀ DIGITALE

Navigare su Internet, in termini di privacy, è simile a guidare un'auto. Ogni veicolo ha una targa che lo identifica e, se compie una violazione, è facile risalire al proprietario. Allo stesso modo, quando navighiamo online, il nostro "identificativo" è l'indirizzo IP, che è assegnato dal nostro provider di connessione (come Telecom, Fastweb, Wind). Questo indirizzo è unico per il dispositivo che stiamo utilizzando per connetterci a Internet.

Ogni volta che accediamo a un sito web o utilizziamo un'applicazione, il nostro dispositivo pubblica una connessione con il server che ospita quel sito. Durante questa connessione, il server riceve il nostro indirizzo IP, il quale può essere utilizzato per identificare la nostra posizione o, in casi estremi, per risalire alla nostra identità. Anche i programmi di posta elettronica, le chat, e le app mobili fanno lo stesso: ogni interazione con il server rivela il nostro IP.

L'indirizzo IP è assegnato in modo casuale dal provider di connessione e, in alcuni casi, può essere dinamico, cioè, cambia ogni volta che ci colleghiamo a Internet. Questo significa che non possiamo scegliere il nostro indirizzo IP, ma è comunque un'informazione che può essere utilizzata per rintracciarci.

Tuttavia, nel caso di azioni online, l'indirizzo IP può essere un elemento importante per identificare chi ha commesso un illecito.

## PRIVACY

*"Diritto alla riservatezza delle informazioni personali e della propria vita privata"*

*art.1 D.lgs n.196/2003*

Per dato personale si intende "qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale". I dati personali si dividono in tre categorie (art. 4 D.lgs 196/2003):

- **DATI SENSIBILI**: "i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale"
- **DATI IDENTIFICATIVI**: "i dati personali che permettono l'identificazione diretta dell'interessato". Sono dati personali, ad esempio, il nome e cognome, l'indirizzo, il codice fiscale, dati sanitari, bancari ma anche la foto o la registrazione della voce
- **DATI GIUDIZIARI**: "i dati personali idonei a rivelare provvedimenti (di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n.313) in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato (ai sensi degli articoli 60 e 61 del codice di procedura penale)"

## PARENTAL CONTROL (SISTEMI DI CONTROLLO PARENTALE – SCP)

Dal 21 novembre 2023, sono ufficialmente entrate in vigore le **linee guide approvate dall'Autorità per le Garanzie nelle Comunicazioni** (AGCOM) in materia di sistemi di protezione dei minori su Internet, che obbligano gli operatori di telefonia a mettere a disposizione dei propri clienti servizi gratuiti di Parental Control per bloccare l'accesso a contenuti online ritenuti non appropriati per i minori di 18 anni.

**Il genitore è tenuto a comunicare all'operatore telefonico che la scheda SIM è in uso a un minore.**

Secondo le disposizioni dell'AGCOM, in particolare, i fornitori di servizi di accesso ad Internet (ISP, Internet Service Provider), a prescindere dalla tecnologia utilizzata per l'erogazione del servizio, sono tenuti a predisporre i cosiddetti Sistemi di Controllo Parentale (SCP), ovvero di sistemi che permettono di limitare o bloccare l'accesso a determinate attività online da parte di un minore, filtrando contenuti ritenuti inappropriati o riservati ad un pubblico di età superiore ai 18 anni.

**I Sistemi di Controllo Parentale sono: gratis, inclusi e attivati dai vari operatori telefonici nelle offerte dedicate ai minori.**

Tra i contenuti che verranno bloccati, nel dettaglio, sono compresi tutti quelli che rientrano nelle categorie oggetto di filtro individuate dall'Autorità, che includono: "Contenuti per adulti", "Gioco d'azzardo e/o scommesse", "Armi", "Violenza", "Odio e discriminazione", "Promozione di pratiche che possono danneggiare la salute alla luce di consolidate conoscenze mediche", "Anonymizer", "Sette".

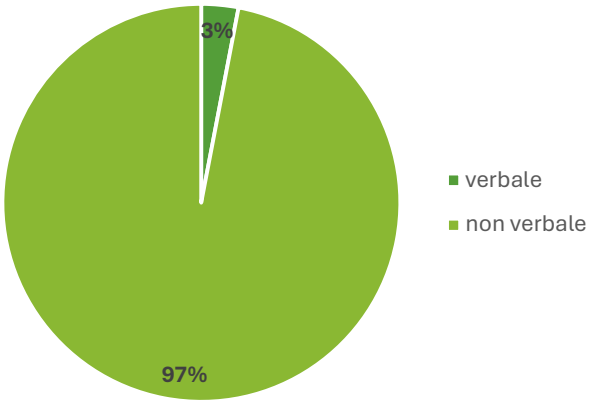
### Alcuni utili consigli

- Nessun sistema di filtraggio, in quanto mezzo "meccanico" può sostituire la **presenza del genitore** e può bloccare tutto il contenuto pericoloso o indesiderato per un bambino o un ragazzo. La supervisione del genitore è necessaria sempre!
- È importante sapere che i filtri sui video e sulle immagini agiscono pochissimo, mentre funzionano meglio sui testi.
- L'uso degli strumenti e dei social accessibili ad un minore devono avere la supervisione del genitore anche per quanto riguarda ciò che i ragazzi scrivono o condividono. Alcune app non sono pericolose in sé ma può diventare pericoloso l'uso che se ne fa.

## COMUNICAZIONE VS CONVERSAZIONI ONLINE

La comunicazione può essere:

- **VERBALE**: parole
- **NON VERBALE**: sguardi, gesti, contatto fisico, vicinanza, contatto oculare, silenzio, tono e ritmo della voce




**Tutte le nostre conversazioni online sono prive della componente non – verbale**.

Il significato del messaggio potrebbe essere diverso per chi scrive rispetto a chi legge.

- Pensare molto prima di scrivere online
- Pensare a quello che il ns interlocutore potrebbe aver inteso
- Preferire conversazioni private che quelle di gruppo

**Esercitarsi nella comunicazione nella vita reale**
**Conoscere la Netiquette**

## DECALOGO

1. Informatevi sul funzionamento della rete
2. Informatevi sull'uso adeguato:
    a. del www (World Wide Web)
    b. della posta elettronica
    c. delle chat
    d. dei Blog
3. Controllate che i giochi online che tanto piacciono ai bambini/ragazzi siano adatti alla loro età (PEGI)
4. Stabilite regole
5. Insegnate la prudenza
6. Proteggete i minori dall'esposizione precoce a materiale pornografico
7. Utilizzate i Parental Control
8. Vigilate: niente può sostituire la vostra presenza!
9. In caso di bullismo o cyberbullismo non esitate a contattare la Scuola e/o a denunciare
10. Educate alla gentilezza nei rapporti e nella comunicazione e al rispetto nella vita reale e in quella virtuale




***"Se potete scegliere tra essere giusti ed essere gentili, siate gentili" Cit. Wonder***

https://www.youtube.com/watch?v=n87nAKMAU50