

## Consigli ai ragazzi per una navigazione sicura in rete

1. Non dare mai informazioni personali (nome, indirizzo, numero di telefono, età, nome e località della scuola o nome degli amici) a chi non conosci personalmente o a chi incontri sul web;
2. Non condividere le tue password con gli amici, ma solo con i tuoi genitori;
3. Cerca di creare password originali, sempre diverse con caratteri numerici e di lettere intervallati tra loro;
4. Non accettare incontri di persona con qualcuno conosciuto online;
5. Non rispondere a messaggi che possano destare confusione o disagio;
6. Non usare un linguaggio offensivo o mandare messaggi volgar online;
7. Se qualcuno usa un linguaggio offensivo con te, parlane con un adulto;
8. Quando usi i social pensa prima di taggare qualcuno, controlla i post in cui sei taggato prima di renderli pubblici, per evitare spiacevoli contenuti sul tuo profilo.
9. Attento ai falsi messaggi: diffida dai messaggi inquietanti, suppliche di aiuto, offerte, richieste di informazioni, avvisi di presenza di Virus in quanto possono essere stratagemmi criminosi;
10. Prudenza con chi non conosci sul web: Non tutti sono davvero chi dicono di essere. Evita di accettare amicizie online da persone sconosciute.
11. Segnala i contenuti che ritieni essere inappropriati o illegali. Di fronte ad un contenuto che ritieni inadeguato segnalalo prontamente ai tuoi genitori o ai tuoi insegnanti;
12. Presta sempre attenzione a ciò che pubblichi in rete: ogni cosa che metti online è sicuramente destinata a rimanere lì per sempre;
13. Non tutti quelli che aggiungi agli amici sono tuoi amici; ricorda che gli amici veri sono quelli che conosci personalmente;
14. Comportarsi da bullo in rete può far soffrire tanto quanto nella vita reale: non usare la rete per mentire, deridere o ingannare. Non alimentare conversazioni che possono nuocere agli altri. Cerca di essere leale e sincero. Non minacciare o prevaricare i più deboli.
15. Non permettere agli amici di condividere informazioni private che ti riguardano senza il tuo consenso: a tua volta non caricare immagini o video che riguardano altre persone, senza che queste abbiano dato, preventivamente, la propria autorizzazione. Soprattutto non inviare o richiedere foto, filmati o messaggi violenti o a sfondo sessuale.



16. Attenzione a quando scarichi qualcosa. Se manca l'autorizzazione del proprietario, o comunque della persona che ne detiene i diritti d'autore, contraffare, copiare e divulgare altrui elaborati (articoli, foto, audio, video...) è soggetto alla legge sulla violazione dei diritti d'autore o del copyright e può essere configurato come un reato.
17. Non condividere i tuoi dati personali. Prima di mettere il tuo numero di telefono o indirizzo online devi essere sicuro devi essere sicuro di sapere dove lo stai postando e perché.

## **Consigli ai genitori per una navigazione in internet dei minori sicura e consapevole**

1. Affiancate i più piccoli sin dalle prime navigazioni in rete in modo da capirne gli interessi e fornire consigli sui siti da evitare e su quelli che, invece, si possono visitare in sicurezza.
2. Non lasciate i bambini e i ragazzi da soli a navigare troppe ore su internet: stabilite quanto tempo possono passare navigando per limitare l'esposizione ai rischi della Rete.
3. Insegnate l'importanza di mantenere riservata l'identità in rete: spiegategli che è importante non fornire dati personali come nome, cognome, età, indirizzo, numero di telefono, nome e orari della scuola, nome degli amici ad altri utenti di siti e social network, sia a garanzia della loro tutela che per quella della propria famiglia.
4. Cercate di stare vicino ai bambini/ragazzi quando creano profili personali sui social network: valutate insieme quale foto sia migliore per il profilo, selezionate insieme le impostazioni di privacy scegliendo con accuratezza a chi saranno visibili i contenuti con divisi in rete, limitate la pubblicazione di contenuti/informazioni troppo personali.
5. NB: la gran parte dei social network prevede, quale età minima per l'iscrizione ai social network, 13 anni.
6. Spiegate ai bambini/ragazzi che può essere pericoloso compilare moduli on line e dite loro di farlo solo dopo avervi consultato.
7. Dite ai bambini/ragazzi di non rispondere alle provocazioni sui social e nelle chat; invitateli a non usare un linguaggio volgare, inappropriato, aggressivo e a comportarsi correttamente in rete.
8. Qualora vostro figlio sembri non interessato a internet, ai social o agli smartphone spiegategli comunque come navigare in sicurezza: stimolato da amici o conoscenti o per mera curiosità, potrebbe avere voglia di usare questi strumenti ed è utile che conosca le forme principali di tutela.
9. Se avete un computer fisso, collocatelo in una stanza centrale della casa piuttosto che nella camera dei ragazzi, per poter controllare in maniera discreta i contenuti visitati. Se invece avete tablet o smartphone, stabilite la semplice regola di consentirne l'uso in una zona centrale della casa in modo da sorvegliare senza far sentire vostro figlio "sottocontrollo".
10. Leggete le e-mail e i messaggi sui social dei minori più piccoli, visionando anche gli allegati. Se non conoscete il mittente non aprite i messaggi né eventuali allegati: questi possono contenere virus o spyware in grado di alterare il funzionamento del vostro dispositivo. Date le stesse indicazioni ai ragazzi più grandi.

11. Insegnate ai vostri figli di non acconsentire alle richieste di incontrare personalmente chi hanno conosciuto in Rete. Spiegate loro che le persone conosciute in chat o sui social network utilizzano, molto spesso, identità false per poter entrare in contatto con i minori e approfittare della loro buona fede.
12. Spiegate ai ragazzi che ciò che fanno su internet non rimane anonimo ma lascia tracce informatiche che permettono di risalire agli autori delle condotte in rete.
13. Stabilite quanto tempo possono passare navigando su Internet.
14. La migliore garanzia di tutela per i minori, in generale, è non lasciarli soli in un ambiente popolato da adulti come la Rete.

**Fonte: Polizia Postale – Sportello sicurezza utenti sul web (<http://www.commissariatodips.it/>)**



## Consigli per un uso sicuro dello smartphone

1. Spiega a tuo/a figlio/a che il telefonino è un mezzo di comunicazione che impone cautela, soprattutto se naviga in rete.
2. Ricordagli/le che foto e riprese effettuate con il telefonino sottostanno alla normativa italiana in materia di protezione della privacy delle persone: se creano immagini o video di persone non sono autorizzati a condividerli, diffonderli nei gruppi di chat, pubblicarli sui socialnetwork. Una volta immessi in rete, foto e filmati possono continuare a essere diffusi senza controllo, per un tempo potenzialmente infinito.
3. Scegli per i tuoi figli SIMCard ricaricabili in modo da poter monitorare il traffico telefonico e di dati di tuo/a figlio/a.
4. Al momento dell'attivazione della SIMCard fornisci ai tuoi figli il PIN ma, preferibilmente, non il PUK. Con il PUK infatti potrai accedere al telefono anche se il pin è stato modificato.
5. Spiega ai tuoi figli che promesse di ricariche facili o altri vantaggi immotivati provenienti da sconosciuti sono spesso tipiche di chi usa la rete con cattive intenzioni.
6. Parla ai tuoi figli della potenziale pericolosità nell'accettare amicizie virtuali o nello scambiare messaggi con utenti sconosciuti: la rete è popolata anche da persone interessate a rapporti sessuali con minorenni, ben consapevoli dell'attrazione che il web esercita sui ragazzi e di quanto i giovani siano poco riservati e cauti nei contatti "virtuali".

**Fonte: Polizia Postale –Sportello sicurezza utenti sul web (<http://www.commissariatodips.it/>)**





Marzo 2021



**GPDP**

**GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI**

# Tutele per i minori vittime di cyberbullismo su social network e web



## Nuove tutele per i minori vittime di cyberbullismo su social network e web

### 1. DI CHE PARLIAMO?

Con il termine «**cyberbullismo**» si intende qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali realizzati, **per via telematica, a danno di minori**, nonché la diffusione di contenuti on line riguardanti uno o più componenti della famiglia di un minore con lo scopo di isolarlo, attaccarlo o metterlo in ridicolo.



### 2. COSA PREVEDE LA LEGGE n. 71/2017?

La nuova legge consente ai minori di chiedere l'oscuramento, la rimozione o il blocco di contenuti, a loro riferiti e diffusi per via telematica, che ritengono essere atti di **cyberbullismo** (ad esempio, foto e video imbarazzanti o offensive, oppure pagine web o post sui social network in cui si è vittime di minacce, offese o insulti, ecc.).

### 3. COME SI PUÒ AGIRE?

Le richieste di cancellazione dei contenuti vanno inviate al titolare del trattamento o al gestore del sito internet o del social media dove sono pubblicate le informazioni, le foto, i video, ecc. ritenuti atti di cyberbullismo. L'istanza può essere inviata **direttamente dal minore, se ha più di 14 anni**, oppure da chi esercita la responsabilità genitoriale.

### 4. COSA SUCCEDDE DOPO CHE LA RICHIESTA E' STATA INVIATA?

Il titolare del trattamento o il gestore del sito internet o del social media che ospita i contenuti ritenuti offensivi risponde ed eventualmente provvede alla richiesta di eliminazione nei tempi previsti dalla legge. Nel caso la richiesta non venga soddisfatta, ci si può rivolgere al Garante per la protezione dei dati personali, che entro 48 ore provvede in merito alla segnalazione. Nei confronti di chi non rispetta le misure disposte dall'Autorità potranno essere applicate le sanzioni previste dal Codice privacy. Per inoltrare le segnalazioni si può utilizzare il modello disponibile su [www.garanteprivacy.it/cyberbullismo](http://www.garanteprivacy.it/cyberbullismo), inviandolo via e-mail a: [cyberbullismo@gpdp.it](mailto:cyberbullismo@gpdp.it).

La scheda presenta una sintesi della legge n. 71/2017 ed ha mere finalità divulgative