

# Privacy e nuove tecnologie a scuola

## Risposte alle domande più frequenti



**Generazioni  
Connesse**  
SAFER INTERNET CENTRE

# Come posso proteggere i miei dati quando utilizzo lo smartphone e il tablet?

Imposta il codice PIN e preferibilmente anche il codice di blocco in modo che non siano facilmente identificabili.

Conservare il codice IMEI utilizzabile per bloccare a distanza l'accesso al tuo smartphone o tablet in caso di furto o smarrimento.

Installare un software di sicurezza antivirus/antimalware, se possibile: essi sono vulnerabili più di un pc.

Quando si naviga in internet utilizzando connessioni wifi pubbliche, assicurarsi che la navigazione sia protetta con protocolli di scambio dati criptati e che l'autenticazione ai siti che si visitano, utilizzino il protocollo Https (cioè http sicuro) perché è un protocollo di trasporto sicuro e previene gli attacchi hacker.

Non conservare nello smartphone password personali, codici di accesso e dati bancari.

Prima di dismettere un cellulare, un tablet o un PC i dati devono essere completamente cancellati: si può ripristinare le impostazioni di fabbrica, rimuovere la scheda sim e la scheda di memoria ed eliminare tutti i backup.

Quando si scaricano applicazioni evitare fonti sconosciute e utilizzare market ufficiali. Verificare che l'applicazione installata non richieda l'accesso ai dati personali (es. foto, rubrica...). Leggere attentamente le condizioni d'uso per evitare di pagare servizi non richiesti o vedere sposte le informazioni personali.

Leggere con attenzione tutte le notifiche di accesso agli account, le notifiche sulle impostazioni di sicurezza e privacy.

# Come faccio a scegliere una password sicura?

Utilizza i nomi di fantasia e non nomi reali perché esistono dei programmi che, utilizzando dizionari on line, possono individuare facilmente il nome che hai scelto per la tua password. Combina insieme maiuscole e minuscole, lettere, numeri e simboli.

È importante cambiare la propria password periodicamente, non salvarla nel cellulare e non rivelarla a nessuno.

È importante non utilizzare la stessa password per account e siti diversi (es. profilo facebook e posta elettronica): in caso di violazione su uno di essi, l'accesso non autorizzato automaticamente si potrebbe estendere agli altri.

# Se si verificano tra gli studenti comportamenti fastidiosi, offensivi su social network o su uno dei sistemi di messaggistica (es. whatsapp, Skipe, Messenger), come può intervenire la scuola?

Il vademecum “la scuola a prova di privacy” del Garante suggerisce agli studenti di avvisare compagni, professori e famiglie se ci si rende conto di essere insultati o messi sotto pressione da altri compagni o da sconosciuti.

La scuola non si può definire estranea ai fatti che accadono agli studenti e ha l’obbligo di aiutare lo studente a risolvere il problema.

Si può chiedere al gestore del social network di intervenire cancellando testi o immagini inappropriate.

# Si possono usare smartphone e tablet a scuola?

Il vademecum “La scuola a prova di privacy” spiega che in generale l’utilizzo di telefoni cellulari, di apparecchi per la registrazione di suoni e immagini è consentito, ma *“esclusivamente per fini personali e sempre nel rispetto dei diritti e delle libertà fondamentali delle persone coinvolte in particolare nella loro immagine e dignità”*.

**Le Istituzioni scolastiche hanno comunque la possibilità di regolare o di inibire l’utilizzo di registratori, smartphone, tablet e altri dispositivi elettronici all’interno delle aule o delle scuole stesse.**

# Come posso fare pubblicità su Internet, assolvere agli obblighi di trasparenza senza violare la privacy?

Il vademecum “la scuola a prova di privacy” del Garante specifica che *“è necessario che gli istituti scolastici prestino particolare attenzione a non rendere accessibili informazioni che dovrebbero restare riservate o a mantenerle online oltre il tempo consentito”*.

Il Garante per facilitare una corretta applicazione della normativa ha predisposto apposite linee guida in materia di trattamento di dati personali.

# Quali regole generali posso tenere a mente quando navigo in rete?

Non pubblicare informazioni personali e dati sensibili di altri utenti e non rendere pubblico un messaggio privato senza l'autorizzazione dell'autore, sia quando sei su un social (chiedi ad es. il consenso prima di taggare con foto e video) sia quando utilizzi mms o sistemi di messaggistica istantanea ( es. wathasapp o messenger).

Non pubblicare foto che potrebbero mettere in una posizione di imbarazzo amici o in generale altri utenti.

Prima di diffondere informazioni accertati che siano esatte, verificale prima.

Quando pubblichi foto, video, frasi o parli di un libro, cita sempre la fonte o metti il link di riferimento.

Quando chiedi l'amicizia a qualcuno su un social che non è tuo amico, motiva la tua richiesta di amicizia.

# Grazie dell'attenzione



**Generazioni  
Connesse**  
SAFER INTERNET CENTRE