Docenti e privacy

Un vademecum per orientarsi tra disposizioni, regolamenti e modelli virtuosi di comportamento professionale

In tempi di regolamenti stringenti, social media, comunicazioni istantanee e rischi sociali, essere docenti non è un compito semplice; in questo breve opuscolo abbiamo riunito alcune "regole" di comportamento e alcuni suggerimenti per aiutare tutti i docenti ad affrontare con consapevolezza e serenità questo passaggio importante nella loro carriera.

FOTOGRAFIE

- Posso scattarle solo agli alunni le cui famiglie hanno preventivamente dato il **consenso**
- Il consenso è specifico! Devo stare attento a dove pubblico le fotografie scattate; può succedere che una famiglia abbia acconsentito alla pubblicazione negli spazi della classe, ma non negli spazi collettivi dell'istituto sul sito
- Salvo casi particolari e vagliati individualmente dal Dirigente Scolastico, sul **sito della scuola** è bene non pubblicare foto degli studenti

RIPRESE VIDEO E FILMATI

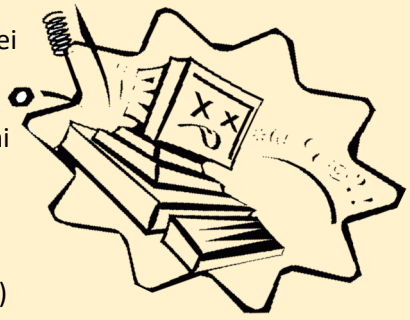
Valgono le stesse regole dettate per le fotografie.

Sebbene spesso siano le stesse famiglie a richiedere o apprezzare l'invio di foto e video presi durante le attività scolastiche, è sempre bene ricordare che il GDPR e il Garante per la Privacy raccomandano cautela e invitano a raccogliere sempre un **consenso informato** da parte dei tutori.

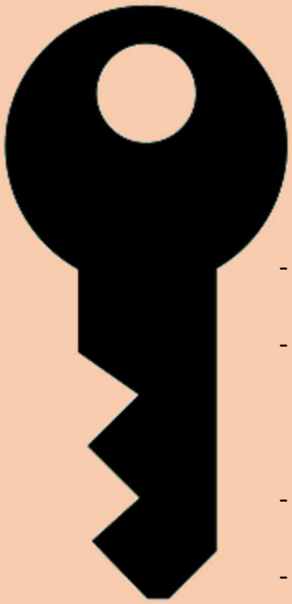
COMPUTER, LIM, LABORATORI INFORMATICI

Occorre vigilare e verificare che venga fatto un uso corretto dei dispositivi informatici in dotazione all'Istituto. In particolare:

- **Sorvegliare** la navigazione in internet, soprattutto dei minorenni
- Chiedere che vengano predisposti **strumenti centralizzati** di:
  - Monitoraggio e controllo della navigazione
  - Blocco dei contenuti inappropriati
- Non lasciare **incustoditi** i dispositivi (intervallo, cambio ora, etc.)
- Verificare che non venga alterata la **configurazione** dei dispositivi



PASSWORD E CREDENZIALI DI ACCESSO

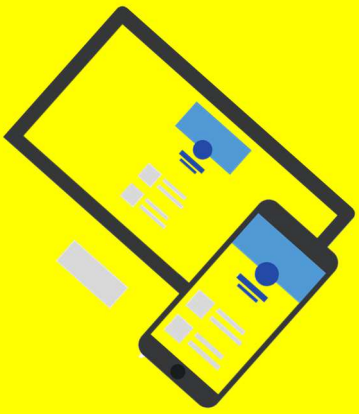


Le credenziali di accesso ai siti, al Registro Elettronico, al sito Istituzionale, alla vostra posta elettronica, vi identificano come gli autori materiali delle operazioni che vengono eseguite una volta entrati. Inoltre, se conosciute, possono dare accesso alle vostre informazioni personali. Per una gestione consapevole della propria identità digitale occorre osservare alcuni precisi comportamenti:

- Le proprie password **non vanno memorizzate** in dispositivi pubblici (es: PC di classe, PC della sala professori, etc)
- Se vi accorgete che una password è rimasta memorizzata dove non dovrebbe, **chiedete aiuto** agli animatori digitali, ai tecnici o all'assistenza informatica del vostro Istituto. Per nessuna ragione lasciate memorizzata la password confidando nella "buona fede" di colleghi e studenti
- Se sussiste anche solo il sospetto che qualcuno conosca la vostra password, **cambiatela** immediatamente
- Non tenete **annotate** le vostre password su foglietti, post-it o agende consultabili da persone non autorizzate

UTILIZZO DI DISPOSITIVI PERSONALI

Prima di utilizzare dispositivi personali a scuola, chiedete se il vostro istituto si è dotato di un **Regolamento per l'utilizzo delle risorse informatiche** e se questo Regolamento contempla delle istruzioni per l'utilizzo di dispositivi personali.



In ogni caso prestate attenzione a quanto viene memorizzato sui vostri dispositivi personali e verificate che sui vostri dispositivi siano presenti almeno:

- Un sistema di autenticazione all'accesso (Password, codice numerico, impronta digitale, etc)
- Un antivirus

DOCUMENTI RISERVATI

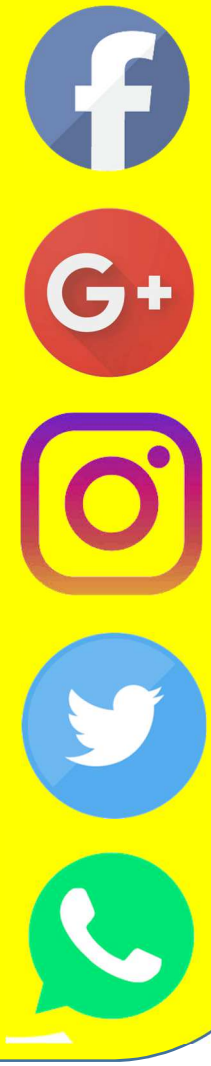
Prima di lavorare su documenti contenenti dati sensibili (PEI, PDP, Relazioni, etc):

- Chiedete se l'Istituto si è dotato di un **Regolamento per l'utilizzo delle risorse informatiche** e se questo prevede istruzioni specifiche
- Informatevi se esistono **strumenti centralizzati** per la gestione di questi documenti (Google Drive di Istituto, spazio apposito nel Registro Elettronico, etc)
- Ricordate che è sempre meglio **non conservare in locale sul proprio dispositivo** documenti riservati e che sarebbe opportuno salvarli in posti appositamente predisposti, configurati, monitorati e protetti

CHIAVETTE USB, HARD DISK ESTERNI

La chiavetta Usb è maneggevole e facilissima da trasportare, ma è altrettanto facile **smarrirla** o **dimenticarla** da qualche parte. Si tratta di un inconveniente che può essere **grave** se per caso conteneva **documenti importanti o personali**. Se possibile, utilizziamo servizi come **Google Drive** o **Dropbox** e se dobbiamo utilizzare una chiavetta USB, cerchiamo i modelli dotati di ganci o anelli che ne consentano il **fissaggio** a borse o portachiavi: in questo modo ridurremo il rischio di smarrimento. Una buona idea è dotare la chiavetta di un **software di sicurezza** basato su crittazione dei dati e protezione con password. Due buoni programmi sono TrueCrypt e Androsa File Protector

UTILIZZO DEI SOCIAL (FACEBOOK, INSTAGRAM, WHATTSAPP, YOUTUBE)



Prima di condividere materiale relativo alla tua scuola, ricorda che:

- non esiste più una separazione tra la **vita "on-line" e quella "off-line"**. Quello che scrivi e le immagini che pubblichi sui social network hanno quasi sempre un riflesso diretto sulla tua vita di tutti i giorni, e nei rapporti con amici, familiari, compagni di classe, colleghi di lavoro. Ed è bene ricordare che l'effetto può non essere necessariamente immediato, ma ritardato nel tempo
- quando inserisci i tuoi dati personali su un sito di social network, ne **perdi il controllo**. I dati possono essere registrati da tutti i tuoi contatti e dai componenti dei gruppi cui hai aderito, rielaborati, diffusi, anche a distanza di anni.
- impara a **distinguere** chi aggiungi alla tua rete di "amici" in base all'uso che ne fai. Se il social network a cui sei iscritto te lo consente, decidi quali tipi di informazioni possono essere consultate dai differenti tipi di amici
- occorre tenere ben **separati i canali di comunicazione ufficiali** (sito istituzionale, Registro Elettronico, etc), sui quali possono essere veicolati contenuti come circolari o avvisi, **dai canali social**, che non necessariamente rispecchiano la linea dell'Istituto e che non devono essere considerati fonti di comunicazioni ufficiali. E' opportuno sottolineare questa differenza a tutti i fruitori dei social: genitori, alunni, docenti
- è opportuno verificare se il tuo Istituto si è dotato di un **Regolamento per l'utilizzo di internet e degli strumenti di comunicazione** social

APPROFONDIMENTI

Il Garante della Privacy ha preparato alcuni vademecum che meritano di essere consultati ed eventualmente pubblicizzati in classe:

- Come tutelarsi nell'era dei social network (link web)
- Social Privacy (PDF)
- E-State in privacy (link web)

CYBERBULLISMO

Il cyberbullismo è una forma di prepotenza virtuale attuata attraverso l'uso di internet e delle tecnologie digitali. Come il bullismo tradizionale è una forma di prevaricazione e di oppressione reiterata nel tempo, perpetrata da una persona o da un gruppo di persone più potenti nei confronti di un'altra percepita come più debole, in genere nel gruppo dei pari.

Caratteristiche del cyberbullismo:

- L'impatto: la diffusione di materiale tramite internet è incontrollabile e non è possibile prevederne i limiti (anche se la situazione migliora, video e immagini potrebbero restare online).
- La possibile anonimità: chi offende online potrebbe tentare di rimanere nascosto dietro un nickname e cercare di non essere identificabile.
- L'assenza di confini spaziali: il cyberbullismo può avvenire ovunque, invadendo anche gli spazi personali e privando l'individuo dei suoi spazi-rifugio (la vittima può essere raggiungibile anche a casa).
- L'assenza di limiti temporali: il cyberbullismo può avvenire a ogni ora del giorno e della notte.
- L'assenza di empatia: non vedendo le reazioni della sua vittima alle sue aggressioni, il cyberbullo non è mai totalmente consapevole delle conseguenze delle proprie azioni e questo ostacola ancor di più la possibilità per lui di provare empatia - o rimorso a posteriori -, per ciò che ha fatto, se non viene aiutato ad esserne consapevole da un amico, da un insegnante o da altri.

E' evidente che tale meccanismo sia possibile con ancora più evidenza se ci si trova ad agire online ed è strettamente collegato all'assenza di empatia (o alla difficoltà di provare empatia), alla difficoltà à di entrare in relazione con l'emotività propria e altrui, una relazione che "la presenza fisica" rende invece più facile da realizzarsi. Questo meccanismo non riguarda appunto solo l'autore si un atto di cyberbullismo, ma anche il gruppo che vi assististe (o che vi partecipa, l'effetto è lo stesso). Questo aspetto fornisce spunti per un **lavoro educativo** che miri invece a rafforzare la consapevolezza, l'assunzione di responsabilità, l'impegno o morale (vs disimpegno) appunto, perché il gruppo può avere un ruolo invece estremante positivo.

Tutti quelli che partecipano anche solo con un like o un commento diventano, di fatto, **corresponsabili** delle azioni del cyberbullo facendo accrescere la portata dell'azione; mettere un "like" su un social network, commentare o condividere una foto o un video che prende di mira qualcuno o semplicemente tacere pur sapendo, mette ragazzi e ragazze nella condizione di avere una responsabilità.

Ma d'altro canto sono proprio loro che possono "fare la differenza" perché la responsabilità è condivisa: il gruppo "silente" che partecipa senza assumersi la responsabilità, rappresenta, in realtà, anche l'elemento che può fermare una situazione di cyberbullismo. E questo appunto costituisce un gancio educativo.

Alcuni link utili:

- Garante Privacy: nuove tutele per i minori
- MIUR: linee di orientamento

COSA FARE IN CASO DI VIOLAZIONI DEI DATI PERSONALI?

La prevenzione è l'arma migliore per evitare violazioni dei dati personali che ci troviamo a trattare, ma a volte da sola non è sufficiente.

Se ci accorgiamo che alcuni dati personali o sensibili che stiamo trattando sono stati sottratti, sono andati smarriti, sono finiti (o possono essere finiti) in mano a persone non titolate per trattarli, occorre:

1) **Non perdere la calma**. In questi casi è molto utile avere una sequenza di azioni da compiere già stabilite a priori: non dovrò così perdere tempo per predisporre un piano di azione, che potrebbe essere inficiato dal mio stato emotivo
2) Analizzare l'evento e cercare di **raccogliere più informazioni possibili**:
    a. Quantità di dati sottratta
    b. Numero di persone coinvolte
    c. Probabilità che qualcuno possa venirne in possesso
3) **Non vergognarsi**. Errori sono commessi da tutti, tutti i giorni. Il fatto che sia capitato a noi non ci rende insegnanti peggiori o cittadini di serie B
4) **Comunicare il fatto** al Dirigente e al DPO: sapranno ascoltarvi senza giudicarvi e prenderanno le contromisure migliori per fronteggiare il problema

ATTENZIONE!

L'errore che più grande che possiamo commettere è pensare che "*tutto si aggiusterà*" e che per quieto vivere non ci conviene far sapere a nessuno che cosa è accaduto!