
REGOLAMENTO PER UTILIZZO DELLA RETE DELL'ENTE E DEI SOCIAL MEDIA

LINEE DI CONDOTTA SUI SOCIAL MEDIA

La Fondazione riconoscendo l'importanza dei social network quali strumenti di comunicazione, che possono avere un impatto significativo nella promozione dell'istituzione e nella diffusione delle informazioni, ha inteso definire le presenti linee di condotta indirizzate tanto agli amministratori dei canali social delle sedi, quanto agli utenti degli stessi.

Le presenti *policy* tengono conto di quanto previsto nelle *Netiquette guidelines*, dalla Dichiarazione dei diritti in internet (Commissione per i diritti e doveri relativi ad Internet 2015) che si intendono implicitamente applicabili e dalle regole di cui al Codice Etico.

Ricordare sempre di essere rispettosi, trasparenti, prudenti, citare le fonti e affidarsi sempre alla propria intelligenza!

PREMESSA

I dipendenti possono usare i social ad uso professionale avendo però cura di tutelare la reputazione della Fondazione e la riservatezza delle informazioni. La pubblicazione di commenti o la condivisione di contenuti sui social espone alla responsabilità personale e può coinvolgere anche quella dell'Ente; è opportuno quindi rispettare in qualsiasi circostanza l'Ente, i colleghi, gli utenti, i concorrenti, ecc.

Occorre inoltre tutelare sempre la riservatezza delle informazioni ed evitare il rischio di divulgare anche involontariamente delle informazioni riservate; non bisogna mai citare o fare riferimento a partner, utenti o fornitori senza il loro preliminare consenso né rivelare accordi o contratti stipulati. Sui social è molto facile e rapido pubblicare una foto e utilizzare i contenuti di terzi. Attenzione però perché il concetto di diritto d'autore è ampio: pubblicare un'immagine, un video, un documento o un'idea di un'altra persona costituisce una violazione del diritto d'autore. Inoltre, non si può pubblicare la foto di una persona sui social senza averne avuto il preventivo accordo.

Occorre ricordare sempre che nella relazione con i minori e più in generale con i corsisti (anche se maggiorenni), anche tramite i social, occorre mantenere il ruolo di docente/formatore. Tutto ciò che è ambiguo deve essere evitato.

Il regime del rapporto docente/allievo non cambia. Internet non è uno spazio libero ma è soggetto alle stesse regole valide nelle sedi della Fondazione. Di conseguenza, è previsto il divieto per il personale formativo di raggiungere direttamente gli allievi (in particolare minorenni) con telefonate a casa o al cellulare o con messaggi di posta elettronica dalla mail personale, se non in casi particolari espressamente autorizzati dalla direzione e previo consenso dei genitori (o degli esercenti la responsabilità genitoriale).

TITOLO I

PRIVACY, INFORMAZIONI CONFIDENZIALI, COPYRIGHT, RISPETTO DEI TERMINI DEL SERVIZIO

In base alla normativa vigente è vietato postare sui social dell'Ente informazioni di natura personale concernenti le persone (studenti, impiegati, docenti, ecc.). È altresì vietato divulgare attraverso i social network le informazioni confidenziali di cui gli amministratori delle pagine siano a conoscenza in ragione del proprio ruolo nella Fondazione.

Prima di effettuare un post occorre accertarsi preventivamente e con attenzione di non infrangere alcun diritto di proprietà intellettuale.

Nell'utilizzo del social network, rispettare sempre i termini e le condizioni d'uso stabiliti dalla piattaforma usata.

TITOLO II

DOVERI DEGLI AMMINISTRATORI DEI SOCIAL MEDIA ISTITUZIONALI

L'attivazione di siti e pagine sui social network necessita di capacità organizzativa per evitare danni; occorre infatti sempre preventivamente definire un modello di presidio dei social e pubblicare la policy specificando chi siamo, l'obiettivo dell'attivazione del social (cosa faccio e cosa non faccio) e le modalità di coinvolgimento degli stakeholder definendo in modo chiaro come voglio usare gli strumenti. Occorre ricordare sempre che si tratta di comunicazione istituzionale. Chi parla a nome della Fondazione deve essere autorizzato altrimenti ogni commento è personale.

Eventuali profili aperti dalle sedi della Fondazione vanno comunicati alla Direzione Generale da parte dei referenti delle singole sedi per il coordinamento delle attività di comunicazione.

Esigenze di aprire profili ulteriori in seno all'Ente vanno preventivamente comunicati alla Direzione per un'apposita valutazione.

Gli amministratori dei canali social delle singole sedi sono autonomamente responsabili del contenuto pubblicato, nel rispetto delle presenti linee di condotta.

Gli amministratori dei canali social delle sedi (Facebook, Twitter e Youtube, ecc.) sono altresì tenuti a rispettare le strategie e gli obiettivi di comunicazione definiti dall'Ente nel Piano di comunicazione dedicato ai social network, nonché le priorità comunicative via via indicate dalla Direzione.

Prima di pubblicare un contenuto è necessario valutarne attentamente l'opportunità, oltre ad effettuare una preliminare indagine approfondita sulla veridicità e la correttezza delle informazioni riportate nel post.

Gli amministratori possono postare sui social network contenuti esterni all'Ente (comunicati o articoli di altra fonte, citazioni di libri o film, frasi celebri, video ecc.) solo se costituiscono un approfondimento di temi oggetto di comunicazione da parte della Fondazione e solo dopo averne vagliato attentamente la qualità e l'attendibilità.

Le "amicizie" di Facebook, i "following" di Twitter e i link in generale devono altresì essere attentamente valutati in funzione delle finalità istituzionali e delle politiche di comunicazione dell'Ente. In generale gli amministratori devono evitare di creare collegamenti con pagine o profili presenti sui social network dei quali non sia chiara la fonte. Gli amministratori devono monitorare la presenza di profili "fasulli" dell'Ente sui social network e segnalarli periodicamente alle Direzioni.

Anche le risposte ai commenti devono essere scrupolosamente ponderate, prima della loro pubblicazione, in considerazione del fatto che l'amministratore non esprime la sua personale opinione, bensì quella dell'istituzione che rappresenta; pertanto l'amministratore non può inserire riferimenti alla sua esperienza individuale né scrivere in prima persona. Le risposte devono comunque essere sempre rispettose di tutti gli stakeholder dell'Ente e del pubblico in generale.

Tutti i commenti devono essere costantemente monitorati, moderati quando è ritenuto necessario o rimossi quando sono giudicati offensivi o contenenti un linguaggio non consono a un'istituzione.

TITOLO III

UTENTI DEI SOCIAL MEDIA ISTITUZIONALI

I canali social della Fondazione hanno lo scopo di contribuire alla comunicazione e alla diffusione della conoscenza di informazioni, eventi, servizi e opportunità.

Gli utenti sono però invitati ad utilizzare gli strumenti offerti, in modo responsabile, evitando commenti offensivi o volgari e a non sfruttare gli spazi social istituzionali della Fondazione per annunci di natura personale.

In particolare, non sono consentiti:

- il razzismo e ogni apologia dell'inferiorità o superiorità di una razza rispetto alle altre;
- offese alle istituzioni o alla religione di qualunque fede;
- commenti in chiave sarcastica, sacrilega e denigratoria, a prescindere dalla parte;
- atteggiamenti e/o posizioni di contestazione, presi a titolo gratuito, palesemente ostili nei confronti dell'istituzione;
- incitamento al mancato rispetto delle presenti regole miranti alla esclusiva destabilizzazione del normale utilizzo dei social network istituzionali;
- argomenti contrari al buon gusto e alle regole del vivere civile e del democratico confronto.

I commenti che contravvengono alle regole di cui sopra verranno rimossi a cura degli amministratori.

Gli utenti sono inoltre invitati a tenere presente che per le richieste di assistenza o per le segnalazioni di disservizi devono utilizzare gli specifici canali attivati dalla Fondazione.

Poiché esiste la possibilità che gli studenti trovino materiale inadeguato e illegale su internet, la Fondazione ha limitato l'accesso ad Internet mediante filtri per la navigazione e le attività svolte in rete vengono monitorate e tracciate nel rispetto delle vigenti normative sulla privacy. I filtri da solo però non bastano ad eliminare tutti i rischi anche perché è possibile commettere errori o attività illegali su siti perfettamente leciti e perché gli studenti sono in grado di collegarsi a internet senza protezione sia da casa che con il proprio cellulare.

I formatori hanno la responsabilità di guidare gli studenti nelle attività on-line, di stabilire obiettivi chiari nell'uso di internet e di insegnare un uso degli strumenti accettabile e responsabile.

Il presente regolamento si rivolge prioritariamente agli studenti anche se le regole valgono per chiunque richieda l'accesso alla rete wireless delle sedi della Fondazione (compresi i formatori).

Tutti gli utenti devono rispettare scrupolosamente questo regolamento, le leggi vigenti in materia di diritti d'autore e tutela della privacy nonché le specifiche norme penali relative al settore informatico e della comunicazione elettronica, oltre alle disposizioni generali di legge.

PRINCIPI GENERALI

Quando si naviga tra i servizi dei social network bisogna informarsi subito di quali sono i diritti e i doveri dell'utente, leggendo il regolamento, tenendosi aggiornati, esplorando i siti informativi e istituzionali che affrontano queste tematiche.

Se si condividono informazioni personali, bisogna farlo scegliendo con cura che cosa rendere pubblico e cosa rendere privato scegliendo con cura le proprie amicizie e i gruppi a cui aderire e proteggendo la propria identità digitale con password complesse.

Se si condividono elementi multimediali o informazioni che riguardano più persone è necessario avere il permesso di ciascun utente coinvolto prima di effettuare la pubblicazione. Non bisogna pubblicare video girati di nascosto e dove sono presenti persone filmate senza il loro consenso.

Bisogna contribuire a rendere il web un luogo sicuro, pertanto ogni volta che un utente commette involontariamente un abuso o un errore, pubblicando del materiale illecito, non idoneo o offensivo, bisogna contattarlo e fornire le spiegazioni relative alle regole, diffondendo così i principi di sicurezza.

Ogni abuso subito o rilevato nella navigazione, deve essere segnalato tramite i canali e gli strumenti offerti dal servizio indicando i riferimenti per ottenere tempestivamente la rimozione del contenuto (abuso, ora data, utenti e servizio coinvolto).

Prima di trasformare un incidente in una denuncia alle autorità competenti avvalersi delle modalità di segnalazione che non obbliga le parti in causa a conseguenze penali e giudiziarie che possono durare anni.

RELAZIONI TRA PERSONE DI PARI LIVELLO

All'interno dei social si instaurano tante relazioni tra singoli utenti, non veicolate o controllate da intermediari, chiamati rapporti di pari livello. È importante fare attenzione a quali informazioni vengono fornite in questo contesto, evitando di condividere dati personali e di contatto.

Bisogna evitare di scambiare file con utenti di cui non ci si può fidare e in ogni caso, anche quando si conosce l'interlocutore, è necessario verificare sempre l'origine dei file ed effettuare un controllo con un antivirus aggiornato.

Se durante una chat o qualsiasi discussione online, l'interlocutore diviene volgare, offensivo o minaccioso, si deve evitare di fomentarlo, ignorandolo e abbandonando la conversazione.

Quando si riscontra un comportamento riconducibile ad un illecito durante una conversazione privata (tentativo di adescamento, cyberbullismo, ecc.) l'utente può sfruttare gli appositi sistemi di reportistica degli abusi predisposti all'interno del servizio, segnalando tempestivamente il nickname che ha perpetrato l'abuso.

In questi casi può essere conveniente abbandonare non soltanto la conversazione ma anche il profilo personale usato fino a quel momento creandosene uno nuovo.

Quando si usano sistemi di file-sharing è importante evitare di scaricare dei file che possono essere illegali e protetti dai diritti d'autore. Bisogna inoltre fare attenzione e non aprire mai file sospetti. Per motivi di sicurezza l'utilizzo di questi sistemi presso le sedi della Fondazione è vietato.

I sistemi di messaggistica dei Social hanno le stesse regole della posta elettronica quindi è necessario preservare la privacy di tutti, cancellano il mittente o i vari destinatari quando si invia un messaggio a più destinatari che non si conoscano tra loro.

Quando si scambiano contenuti multimediali o si pubblicano video con colonna sonora o musica bisogna essere sicuri di avere il diritto d'uso e di non utilizzare file coperto da copyright.

CONTENUTI GENERATI DAGLI UTENTI

I contenuti pubblicati sulle applicazioni web hanno diversi livelli di visibilità. Pertanto quando si inizia a pubblicare materiale in una community bisogna studiare ed imparare ad utilizzare correttamente le funzioni per l'impostazione dei livelli di privacy. Dal momento che ciò che viene pubblicato su un social è persistente e spesso non è facile da cancellare, bisogna evitare di contribuire con materiale che in futuro non si vorrebbe veder pubblicato.

Quando si contribuisce con del materiale in un ambiente condiviso, l'utente è tenuto ad essere coerente con il contesto e le regole della community, evitando di pubblicare materiale inadeguato che potrebbe essere fuori contesto.

Se si usa un nuovo servizio messo a disposizione dal Social, bisogna informarsi su quali sono gli strumenti per segnalare materiale e comportamenti non idonei, e quali sono le modalità corrette per farlo.

Se un contenuto viene moderato e non è più visibile online, probabilmente non è idoneo!

Quando si fa uso di etichette per catalogare un contenuto, bisogna assicurarsi che sia coerente con il contenuto o che indichi la persona corretta.

LA GESTIONE DELLE RELAZIONI SOCIALI – COMMUNITIES

Le relazioni sociali che si sviluppano all'interno dei Social sono simili a quelle reali, deve essere gestita la fiducia verso i propri contatti proprio come accade nella realtà. Bisogna aggiungere alla rete dei propri amici solo le persone che hanno in vari modi dimostrato di essere affidabili. Conviene gestire la propria privacy quando si aggiungono persone su cui si hanno dubbi.

Se si instaura un'amicizia virtuale con persone di cui non si conosce la reale identità, bisogna evitare di condividere contatti e dati personali e contenuti privati soprattutto se riguardano terze persone.

La rete social non è facile da controllare quindi bisogna ricordare che gli amici degli amici spesso hanno modo di avere accesso a informazioni e contenuti personali anche se ci sono sconosciuti.

Se si ha accesso a comunicazioni private di altri utenti (per errori di impostazioni della privacy da parte dell'utente per esempio) bisogna notificarlo all'utente ed evitare di leggere messaggi privati.

La reputazione digitale è persistente e si diffonde velocemente pertanto non bisogna mai diffamare le persone, soprattutto se le stesse non sono presenti sui social e non possono accorgersi del danno subito.

REGOLE PER UN CORRETTO UTILIZZO DEI SOCIAL MEDIA INTERNI ED ESTERNI E DELLE RETI DELL'ENTE

Ricordare di:

- non usare l'accesso wireless senza autorizzazione
- non cedere gli accessi ad altri
- verificare i propri parametri di riservatezza per essere certi di sapere a chi ci si sta rivolgendo e a chi si dà accesso alle proprie informazioni
- indicare chiaramente nei propri commenti o biografie che non si parla a nome dell'Ente. Se si parla dell'Ente, chiarire che state parlando esclusivamente a vostro nome evitando di usare il noi
- indicare di essere dipendenti della Fondazione se si partecipa, anche a titolo personale, ad un social esterno a noi e si discute di un argomento direttamente collegato all'Ente o alla sua attività
- se si fa riferimento a contenuti provenienti da altri siti, creare un link verso la pagina interessata e citare la fonte
- avvisare la Direzione di riferimento qualora si dovesse individuare una conversazione online in cui la Fondazione, i suoi servizi o i suoi dipendenti/utenti vengono attaccati e lasciar rispondere alle persone autorizzate a comunicare per conto dell'Ente
- non pubblicare comunicazioni commerciali non autorizzate
- non raccogliere contenuti o informazioni degli utenti
- non caricare virus o codici dannosi; mantenere il proprio PC/terminale aggiornato, protetto e pulito da virus e spy-ware
- non cercare di ottenere informazioni di accesso o accedere ad account di altri utenti
- non denigrare, intimidire o molestare altri utenti
- non pubblicare contenuti minatori, pornografici, con incitazioni all'odio o alla violenza
- non sviluppare o utilizzare applicazioni di terzi con contenuti correlati all'alcol, o rivolti a un pubblico adulto senza le dovute restrizioni
- non usare i social per scopi illegali, ingannevoli, malevoli o discriminatori
- non accedere a siti con contenuti inadeguati o vietati
- non svolgere nessuna attività atta a rallentare, controllare, eludere o compromettere la sicurezza della rete in qualsiasi modo
- Alcuni esempi:
 - ❖ attaccare, denigrare o rispondere ad attacchi rischia di creare problemi anziché risolverli. Si raccomanda di rispettare sempre i propri interlocutori
 - ❖ non dimenticare che prendendo pubblicamente posizione si rischia di creare dei conflitti
 - ❖ possono esprimersi a nome dell'Ente solo le persone autorizzate. È quindi possibile esprimere a proprio nome, raccontare un'esperienza ma mai parlare a nome dell'Ente
 - ❖ capire bene che i commenti che si pubblicano o i contenuti che si condividono possono essere accessibili a tutti per un periodo anche molto lungo.

Ricordare che i dati una volta pubblicati escono dal nostro controllo e possono essere rubati, copiati, falsificati.

È sempre necessario rispettare la privacy delle persone. È sempre vietato pubblicare sui propri social network dati, foto, e qualsiasi prodotto multimediale in cui compaiono immagini e commenti che riguardano personale docente e non, strutture dell'ente in qualsiasi contesto formativo.

TITOLO IV REATI E VIOLAZIONI

Alcuni comportamenti, al di là delle regole di buona educazione, talvolta sono solo apparentemente innocui e possono portare a commettere veri e propri reati

Reati informatici (legge 547/93):

- Accesso abusivo ad un sistema informatico e telematico
- Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico
- Danneggiamento informatico
- Detenzione e diffusione abusiva di codici di accesso a sistemi informativi o telematici
- Frode informatica

Reati non informatici

- Ingiuria
- Diffamazione
- Minacce e molestie
- Violazione dei diritti d'autore

TITOLO V

SANZIONI

Le sanzioni nei confronti dei ragazzi sono definite nel regolamento.

In particolare, in caso di uso improprio dei social può essere prevista

- La sospensione di 4 a 5 giorni
- La penalizzazione con un voto sulla scheda di valutazione
- La verifica in tutte le materie

a seconda della gravità del fatto. Spetta al consiglio di classe la definizione della sanzione

Per i provvedimenti disciplinari nei confronti del personale si rimanda dal CCNL.