Documento di ePolicy

BSIC80800X

I. C. F.ROSSELLI ARTOGNE

VIA CAMILLO GOLGI N. 1 - 25040 - ARTOGNE - BRESCIA (BS)

SIMONETTA MARAFANTE

Capitolo 1 - Introduzione al documento di ePolicy

1.1 - Scopo dell'ePolicy

Le TIC (Tecnologie dell'informazione e della comunicazione) rappresentano strumenti fondamentali nel processo educativo e per l'apprendimento degli studenti e delle studentesse.

Le "competenze digitali" sono fra le abilità chiave all'interno del Quadro di riferimento Europeo delle Competenze per l'apprendimento permanente e di esse bisogna dotarsi proprio a partire dalla scuola (Raccomandazione del Consiglio Europeo del 2006 aggiornata al 22 maggio 2018, relativa alle competenze chiave per l'apprendimento permanente).

In un contesto sempre più complesso, diventa quindi essenziale per ogni Istituto Scolastico dotarsi di una E-policy, un documento programmatico volto a promuovere le competenze digitali ed un uso delle tecnologie positivo, critico e consapevole, sia da parte dei ragazzi e delle ragazze che degli adulti coinvolti nel processo educativo. L'E-policy, inoltre, vuole essere un documento finalizzato a prevenire situazioni problematiche e a riconoscere, gestire, segnalare e monitorare episodi legati ad un utilizzo scorretto degli strumenti.

L'E-policy ha l'obiettivo di esprimere la nostra visione educativa e proposta formativa, in riferimento alle tecnologie digitali. Nello specifico:

- l'approccio educativo alle tematiche connesse alle "competenze digitali", alla privacy, alla sicurezza online e all'uso delle tecnologie digitali nella didattica e nel percorso educativo;
- le norme comportamentali e le procedure di utilizzo delle Tecnologie dell'Informazione e della Comunicazione (ICT) in ambiente scolastico;
- le misure per la prevenzione e la sensibilizzazione di comportamenti on-line a rischio;
- le misure per la rilevazione, segnalazione e gestione delle situazioni rischiose legate ad un uso non corretto delle tecnologie digitali.

Argomenti del Documento

Perché è importante dotarsi di una E-policy?

Attraverso l'E-policy il nostro Istituto si vuole dotare di uno strumento operativo a cui tutta la comunità educante dovrà fare riferimento, al fine di assicurare un approccio alla tecnologia che sia consapevole, critico ed efficace, e al fine di sviluppare, attraverso specifiche azioni, una conoscenza delle opportunità e dei rischi connessi

all’uso di Internet.

L’ E-policy fornisce, quindi, delle linee guida per garantire il benessere in Rete, definendo regole di utilizzo delle TIC a scuola e ponendo le basi per azioni formative e educative su e con le tecnologie digitali, oltre che di sensibilizzazione su un uso consapevole delle stesse.

Il presente documento ha lo scopo di illustrare all'utenza scolastica le regole per un uso corretto e responsabile degli strumenti tecnologici collegati alla rete internet in uso nell'Istituto.

Si intende promuovere lo sviluppo della competenza digitale, che passa attraverso la conoscenza di procedure e competenze tecniche e di norme comportamentali, dettate da un uso consapevole e critico da parte degli alunni, delle tecnologie digitali e di internet. Lo scopo è di prevenire ed eventualmente rilevare e affrontare, situazioni derivanti da un uso pericoloso delle stesse.

Il primo passo è informare gli alunni dei rischi cui si espongono nella navigazione in rete, mentre dal canto suo l'Istituto si attiva per limitare l'accesso a siti potenzialmente dannosi, i cui contenuti possano risultare illegali o inadeguati. Gli insegnanti, infine, hanno il ruolo di guidare le attività on-line a scuola e illustrare le regole di comportamento per la navigazione in rete anche a casa.

Ai docenti, in particolare, spetta il ruolo di informare, piuttosto che censurare, gli alunni affinché imparino ad usare consapevolmente i contenuti e i servizi della rete per conoscere gli effetti cognitivi, comportamentali delle sue potenzialità oltre alle informazioni utili a gestire gli strumenti tecnologici.

1.2 - Ruoli e responsabilità

Affinché l’E-policy sia davvero uno strumento operativo efficace per la scuola e tutta la comunità educante è necessario che ognuno, secondo il proprio ruolo, s’impegni nell’attuazione e promozione di essa.

IL DIRIGENTE SCOLASTICO:
- individua attraverso il Collegio dei Docenti un referente del bullismo e cyberbullismo;
- coinvolge, nella prevenzione e contrasto al fenomeno de bullismo, tutte le componenti

della comunità scolastica, particolarmente quelle che operano nell'area dell'informatica, partendo dall'utilizzo sicuro di Internet a scuola;
- prevede all'interno del PTOF corsi di aggiornamento e formazione in materia di prevenzione dei fenomeni di bullismo e cyberbullismo, rivolti al personale docente ed ATA;
- promuove sistematicamente azioni di sensibilizzazione dei fenomeni del bullismo e cyberbullismo nel territorio in rete con enti, associazioni, istituzioni locali ed altre scuole, coinvolgendo alunni, docenti, genitori ed esperti;
- favorisce la discussione all'interno della scuola, attraverso i vari organi collegiali, creando i
presupposti di regole condivise di comportamento per il contrasto e prevenzione dei fenomeni del
bullismo e cyberbullismo;
- prevede azioni culturali ed educative rivolte agli studenti, per acquisire le competenze necessarie
all'esercizio di una cittadinanza digitale consapevole.
IL REFERENTE DEL "BULLISMO E CYBERBULLISMO":
- promuove la conoscenza e la consapevolezza del bullismo e del cyber-bullismo attraverso progetti
d'istituto che coinvolgano genitori, studenti e tutto il personale;
-coordina le attività di prevenzione ed informazione sulle sanzioni previste e sulle responsabilità di
natura civile e penale, anche con eventuale affiancamento di genitori e studenti;
- si rivolge a partner esterni alla scuola, quali servizi sociali e sanitari, associazioni, aziende del
privato sociale, forze di polizia, ecc., per realizzare un progetto di prevenzione;
- cura rapporti di rete fra scuole per eventuali convegni/seminari/corsi e per la giornata mondiale sulla Sicurezza in Internet la "Safer Internet Day".
IL COLLEGIO DOCENTI:
- promuove scelte didattiche ed educative, anche in collaborazione con altre scuole in rete, per la
prevenzione del fenomeno
IL CONSIGLIO DI CLASSE:
- pianifica attività didattiche e/o integrative finalizzate al coinvolgimento attivo e collaborativo degli studenti e all'approfondimento di tematiche che favoriscano la riflessione e la presa di coscienza della necessità dei valori di convivenza civile;
- favorisce un clima collaborativo all'interno della classe e nelle relazioni con le famiglie propone
progetti di educazione alla legalità e alla cittadinanza attiva.
IL DOCENTE:
- intraprende azioni congruenti con l'utenza del proprio ordine di scuola, tenuto conto che l'istruzione ha un ruolo fondamentale sia nell'acquisizione e rispetto delle norme relative alla convivenza civile, sia nella trasmissione dei valori legati ad un uso responsabile di Internet;

- valorizza nell'attività didattica modalità di lavoro di tipo cooperativo e spazi di riflessioni adeguati al
livello di età degli alunni.

I GENITORI:
- partecipano attivamente alle azioni di
formazione/informazione, istituite dalle scuole, sui
comportamenti sintomatici del bullismo e del cyberbullismo;
- sono attenti ai comportamenti dei propri figli;
- vigilano sull'uso delle tecnologie da parte dei ragazzi, con particolare attenzione ai tempi, alle modalità, agli atteggiamenti conseguenti (i genitori dovrebbero allertarsi se uno studente, dopo l'uso di Internet o del proprio telefonino, mostra stati depressivi, ansiosi o paura);
- conoscono le azioni messe in campo dalla scuola e collaborano secondo le modalità previste dal
Patto di corresponsabilità;
- conoscono il codice di comportamento dello studente;
- conoscono le sanzioni previste da regolamento d'istituto nei casi di bullismo, cyberbullismo e
navigazione on-line a rischio.
GLI ALUNNI:
- sono coinvolti nella progettazione e nella realizzazione delle iniziative scolastiche, al fine di favorire un miglioramento del clima relazionale; in particolare, dopo opportuna formazione, possono operare come tutor per altri studenti;
- imparano le regole basilari, per rispettare gli altri, quando sono connessi alla rete, facendo
attenzione alle comunicazioni (email, sms, mms) che inviano;
- non è loro consentito, durante le attività didattiche o comunque all'interno della scuola, acquisire –
mediante telefonini cellulari o altri dispositivi elettronici - immagini, filmati o registrazioni vocali, se non per finalità didattiche, previo consenso del docente.
La divulgazione del materiale acquisito all'interno dell'istituto è utilizzabile solo per fini esclusivamente personali di studio o documentazione e comunque nel rispetto del diritto alla riservatezza di tutti;
- durante le lezioni o le attività didattiche non possono usare cellulari, giochi elettronici e riproduttori di musica, se non per finalità didattiche, previo consenso del docente.

1.3 - Un'informativa per i soggetti esterni che erogano attività educative

nell'Istituto

Tutti gli attori che entrano in relazione educativa con gli studenti e le studentesse devono: mantenere sempre un elevato profilo personale e professionale, eliminando atteggiamenti inappropriati, essere guidati dal principio di interesse superiore del minore, ascoltare e prendere in seria considerazione le opinioni ed i desideri dei minori, soprattutto se preoccupati o allertati per qualcosa.

Sono vietati i comportamenti irrispettosi, offensivi o lesivi della privacy, dell'intimità e degli spazi personali degli studenti e delle studentesse oltre che quelli legati a tollerare o partecipare a comportamenti di minori che sono illegali, o abusivi o che mettano a rischio la loro sicurezza.

Tutti gli attori esterni sono tenuti a conoscere e rispettare le regole del nostro Istituto dove sono esplicitate le modalità di utilizzo dei propri dispositivi personali (smartphone, tablet, pc, etc.) e quelli in dotazione della scuola, evitando un uso improprio o comunque deontologicamente scorretto durante le attività con gli studenti e le studentesse. Esiste l'obbligo di rispettare la privacy, soprattutto dei soggetti minorenni, in termini di fotografie, immagini, video o scambio di contatti personali (numero, mail, chat, profili di social network).

Sono da considerarsi tipologie persecutorie qualificate come bullismo:
- la violenza fisica, psicologica o l'intimidazione del gruppo, specie se reiterata;
- l'intenzione di nuocere;
- l'isolamento della vittima.
Rientrano nel cyberbullismo:
- Flaming: litigi on line nei quali si fa uso di un linguaggio violento e volgare.
- Harassment: molestie attuate attraverso l'invio ripetuto di linguaggi offensivi.
- Cyberstalking: invio ripetuto di messaggi che includono esplicite minacce fisiche, al punto che la
vittima arriva a temere per la propria incolumità.
- Denigrazione: pubblicazione all'interno di comunità virtuali, quali newsgroup, blog, forum di
discussione, messaggistica immediata, siti Internet, ecc., di pettegolezzi e commenti crudeli,
calunniosi e denigratori.
- Outing estorto: registrazione delle confidenze – raccolte all'interno di un ambiente privato - creando
un clima di fiducia e poi inserite integralmente in un blog pubblico.
- Impersonificazione: insinuazione all'interno dell'account diun'altra persona con l'obiettivo di inviare dal medesimo messaggi ingiuriosi che screditino la vittima.
- Esclusione: estromissione intenzionale dall'attività on line.
- Sexting: invio di messaggi via smartphone ed Internet, corredati da immagini a sfondo sessuale.

All’interno della procedura disciplinare, che vale per
qualsiasi comportamento contrario al regolamento di Istituto, si inserisce una parte specifica per gli episodi di bullismo e cyberbullismo in base all’attuale normativa:
- attraverso la compilazione del modulo in formato cartaceo opportunamente predisposto, viene effettuata una segnalazione al referente per il bullismo ed il cyberbullismo che ne dà immediata comunicazione al DS il quale valuta se ricorrono gli estremi per una denuncia; la segnalazione può essere anonima, ma va sempre riportata per iscritto anche se raccolta oralmente;
- nel caso in cui la segnalazione arrivi direttamente al D.S., questi procederà come da prescrizioni
normative;
- diverse ipotesi:
- il fatto non costituisce reato o ipotizza un reato a querela di parte: il D.S. informa tempestivamente i soggetti esercenti la responsabilità genitoriale, ovvero i tutori dei minori coinvolti e attiva adeguate azioni di carattere educativo;
- il D.S. ha notizia di reato: sporge subito denuncia per iscritto all’autorità giudiziaria (Questura, Carabinieri, ecc.), anche quando non sia individuata la persona alla quale il reato è attribuito (art 331 cpp);
- si evidenzia che sia la detenzione che la divulgazione di qualsiasi immagine di tipo sessuale o di esposizione di nudità (prodotto anche attraverso la pratica del “sexting”) è considerato dalla legislazione vigente materiale pedopornografico; è, pertanto, necessario comunicarlo immediatamente al D.S. perché trasmetta la notizia tempestivamente, con relazione circostanziata, alla polizia postale o altra forza di polizia;
- quando un docente o un componente del personale A.T.A. viene a conoscenza di un comportamento ipotizzabile verosimilmente e ragionevolmente come reato ha l’obbligo di
comunicarlo con la massima urgenza al D.S. perché adotti le misure necessarie.

1.4 - Condivisione e comunicazione dell’ePolicy all’intera comunità scolastica

Il documento di E-policy viene condiviso con tutta la comunità educante, ponendo al centro gli studenti e le studentesse e sottolineando compiti, funzioni e attività reciproche. È molto importante che ciascun attore scolastico (dai docenti agli/lle studenti/esse) si faccia a sua volta promotore del documento.

L’E-policy viene condivisa e comunicata al personale, agli studenti e alle studentesse, alla comunità scolastica attraverso:

- la pubblicazione del documento sul sito istituzionale della scuola;
- il Patto di Corresponsabilità, che deve essere sottoscritto dalle famiglie e rilasciato alle stesse all'inizio dell'anno scolastico;

Il documento è approvato dal Collegio dei Docenti e dal Consiglio di Istituto e viene esposto in versione semplificata negli spazi che dispongono di pc collegati alla Rete o comunque esposto in vari punti spaziali dell'Istituto.

Gli studenti e le studentesse vengono informati sul fatto che sono monitorati e supportati nella navigazione on line, negli spazi della scuola e sulle regole di condotta da tenere in Rete.

La condivisione della E-policy avverrà attraverso la pubblicazione sul sito web della scuola, dopo essere stata approvata dal Collegio dei Docenti e dal Consiglio d'istituto. All'inizio del percorso scolastico di ogni ordine di scuola, la E-Policy verrà illustrata ai genitori agli alunni insieme al Patto di Corresponsabilità Educativa.

1.5 - Gestione delle infrazioni alla ePolicy

La scuola gestirà le infrazioni all'E-policy attraverso azioni educative e/o sanzioni, qualora fossero necessarie, valutando i diversi gradi di gravità di eventuali violazioni.

Il Dirigente Scolatico:
a. informa immediatamente e coinvolge i genitori (ad eccezione che per i sospetti casi di
maltrattamento per i quali bisogna segnalare alle Forze dell'Ordine);
b. nel caso di mancata collaborazione della famiglia o della sua inadeguatezza rispetto al caso,
segnala il caso ai Servizi Sociali del Comune e/o alla Tutela Minori;
c. organizza attività di formazione/informazione a favore della comunità scolastica;
d. raccolte le informazioni attraverso l'apposito modulo, il Dirigente Scolastico, informa tempestivamente i genitori dei fatti;
e. in presenza di un testimone e di un genitore in caso di studente/ssa minorenne età, procede a:
- ascoltare i protagonisti dei fatti al fine di acquisire testimonianze e versioni;
- ascoltare i genitori, soprattutto nel caso di minori;
- ricostruire i fatti alla luce di quanto emerso;
- accogliere eventuali documenti o materiali utili anche scritti, consegnati alla scuola da

interessati e controinteressati;

1.6 - Integrazione dell'ePolicy con Regolamenti esistenti

Il Regolamento dell'Istituto Scolastico viene aggiornato con specifici riferimenti all'E-policy, così come anche il Patto di Corresponsabilità, in coerenza con le Linee Guida Miur e le indicazioni normative generali sui temi in oggetto.

La Policy è coerente con quanto stabilito dalla Legge (Statuto delle studentesse e degli studenti della scuola secondaria DPR 24 giugno 1998 n. 249 modificato dal DPR 21 novembre 2007 n. 235; Legge 29 maggio 2017 n. 71 "Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo"; Legge 31 dicembre 1996 n. 675 "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali").

La presente E-Policy prende spunto e in taluni casi è parte integrante del Regolamento d'Istituto approvato nel Collegio Docenti Unitario n. 3 (delibera n.13) del 27 ottobre 2020 e successivamente approvato dal Consiglio d'Istituto n. 1 (delibera n. 1) del 29 ottobre 2020.

1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

L'E-policy viene aggiornata periodicamente e quando si verificano cambiamenti significativi in riferimento all'uso delle tecnologie digitali all'interno della scuola. Le modifiche del documento saranno discusse con tutti i membri del personale docente. Il monitoraggio del documento sarà realizzato a partire da una valutazione della sua efficacia in riferimento agli obiettivi specifici che lo stesso si pone.

L'E-policy verrà aggiornata periodicamente dal gruppo di lavoro e comunque ogni qualvolta ci saranno cambiamenti significativi nelle normative o nell'utilizzo delle nuove tecnologie all'interno della scuola.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

- Organizzare incontri per la consultazione degli studenti/studentesse sui temi dell'ePolicy per cui si evidenzia la necessità di regolamentare azioni e comportamenti.

Azioni da svolgere nei prossimi 3 anni:

- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto agli studenti
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai docenti
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai genitori

Capitolo 2 - Formazione e curricolo

2.1. Curricolo sulle competenze digitali per gli studenti

I ragazzi usano la Rete quotidianamente, talvolta in modo più "intuitivo" ed "agile" rispetto agli adulti, ma non per questo sono dotati di maggiori "competenze digitali".

Infatti, "la competenza digitale presuppone l'interesse per le tecnologie digitali e il loro utilizzo con dimestichezza e spirito critico e responsabile per apprendere, lavorare e partecipare alla società. Essa comprende l'alfabetizzazione informatica e digitale, la comunicazione e la collaborazione, l'alfabetizzazione mediatica, la creazione di contenuti digitali (inclusa la programmazione), la sicurezza (compreso l'essere a proprio agio nel mondo digitale e possedere competenze relative alla cybersicurezza), le questioni legate alla proprietà intellettuale, la risoluzione di problemi e il pensiero critico" ("Raccomandazione del Consiglio europeo relativa alla competenze chiave per l'apprendimento permanente", C189/9, p.9).

Per questo la scuola si impegna a portare avanti percorsi volti a promuovere tali competenze, al fine di educare gli studenti e le studentesse verso un uso consapevole e responsabile delle tecnologie digitali. Ciò avverrà attraverso la progettazione e implementazione di un curricolo digitale.

La scuola ha il dovere di fornire agli studenti l'accesso alle TIC e alla rete, aiutandoli a maturare competenze e strumenti per una consapevole cittadinanza digitale. Per questo l'Istituto si è dotato di un curricolo digitale che prevede il coinvolgimento di tutti gli alunni dell'IstItuto dalla scuola dell'Infanzia alla Secondaria di Secondo grado.
In particolare il curricolo prevede di:
- insegnare ad utilizzare la Rete, rendendo gli alunni consapevoli delle conseguenze delle violazioni;
- mostrare come produrre e pubblicare contenuti digitali in modo adeguato;
- reperire e adeguare i materiali prelevati da Internet per utilizzarli nella didattica, vagliando le informazioni e accertandone la fondatezza;
- imparare a segnalare la presenza di contenuti illeciti.

2.2 - Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica

È fondamentale che i docenti tutti siano formati ed aggiornati sull'uso corretto, efficace ed efficiente delle TIC nella didattica, al fine di usarle in modo integrativo ed inclusivo.

Ciò si rende necessario per fornire agli studenti e alle studentesse modelli di utilizzo positivo, critico e specifico delle nuove tecnologie e per armonizzare gli apprendimenti.

La scuola promuove la partecipazione del personale (Docenti, Assistenti Amministrativi, Collaboratori Scolastici) a corsi, convegni e seminari interni ed esterni all'Istituto, assicurando tempestiva e capillare informazione e agevolando il personale che intenda parteciparvi.

2.3 - Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali

La scuola si impegna a promuovere percorsi formativi per gli insegnanti sul tema dell'uso consapevole delle tecnologie digitali e della prevenzione dei rischi online. Ciò avverrà tramite specifici momenti di aggiornamento che, con cadenza, verranno organizzati dall'Istituto scolastico con la collaborazione del personale specializzato interno (animatore digitale, referente bullismo e cyberbullismo) e se necessario del personale esterno (professionisti qualificati), con il supporto della rete scolastica del territorio (USR, Osservatori regionali sul bullismo, scuole Polo, etc…), delle amministrazioni comunali, dei servizi socio-educativi e delle associazioni presenti.

La scuola, nelle persone del Dirigente Scolatico, del refente del Cyberbullismo e dell'Animatore Digitale, promuove all'interno degli organi collegiali, momenti di confronto e condivisione finalizzati a mettere a disposizione di tutto il corpo docente conoscenze e competenze acquisite dai singoli partecipanti nei diversi corsi. In presenza di appositi fondi la scuola si impegna altresì ad organizzare percorsi formativi specifici.

2.4. - Sensibilizzazione delle famiglie e integrazioni al Patto di Corresponsabilità

Nella prevenzione dei rischi connessi ad un uso non consapevole delle TIC, così come nella promozione di un loro uso positivo e capace di coglierne le opportunità, è necessaria la collaborazione di tutti gli attori educanti, ognuno secondo i propri ruoli e le proprie responsabilità. Scuola e famiglia devono rinforzare l'alleanza educativa e promuovere percorsi educativi continuativi e condivisi per accompagnare insieme ragazzi/e e bambini/e verso un uso responsabile e arricchente delle tecnologie digitali, anche in una prospettiva lavorativa futura. L'Istituto garantisce la massima informazione alle famiglie di tutte le attività e iniziative intraprese sul tema delle tecnologie digitali, previste dall'ePolicy e dal suo piano di azioni, anche attraverso l'aggiornamento, oltre che del regolamento scolastico, anche del "Patto di corresponsabilità" e attraverso una sezione dedicata sul sito web dell'Istituto.

Le famiglie hanno sottoscritto il Patto educativo di corresponsabilità. Firmando questo documento si sono impegnate ad accompagnare e supervisionare i figli durante la navigazione in rete. La scuola sostiene i genitori organizzando incontri ed eventi sui temi dell'uso consapevole della rete e delle tecnologie dell'informazione.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2019/2020)

- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.

AZIONI (da sviluppare nell'arco dei tre anni scolastici successivi)

- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie

digitali.

Capitolo 3 - Gestione dell'infrastruttura e della strumentazione ICT della e nella scuola

3.1 - Protezione dei dati personali

"Le scuole sono chiamate ogni giorno ad affrontare la sfida più difficile, quella di educare le nuove generazioni non solo alla conoscenza di nozioni basilari e alla trasmissione del sapere, ma soprattutto al rispetto dei valori fondanti di una società. Nell'era di Internet e in presenza di nuove forme di comunicazione questo compito diventa ancora più cruciale. È importante riaffermare quotidianamente, anche in ambito scolastico, quei principi di civiltà, come la riservatezza e la dignità della persona, che devono sempre essere al centro della formazione di ogni cittadino".

(cfr. http://www.garanteprivacy.it/scuola).

Ogni giorno a scuola vengono trattati numerosi dati personali sugli studenti e sulle loro famiglie. Talvolta, tali dati possono riguardare informazioni sensibili, come problemi sanitari o particolari disagi sociali. Il "corretto trattamento dei dati personali" a scuola è condizione necessaria per il rispetto della dignità delle persone, della loro identità e del loro diritto alla riservatezza. Per questo è importante che le istituzioni scolastiche, durante lo svolgimento dei loro compiti, rispettino la privacy, tutelando i dati personali dei soggetti coinvolti, in particolar modo quando questi sono minorenni.

La protezione dei dati personali è un diritto fondamentale dell'individuo ai sensi della Carta dei diritti fondamentali dell'Unione europea (art. 8), tutelato dal Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 (relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati).

Anche le scuole, quindi, hanno oggi l'obbligo di adeguarsi al cosiddetto GDPR (General Data Protection Regulation) e al D.Lgs. 10 agosto 2018, n. 101, entrato in vigore lo scorso 19 settembre.

In questo paragrafo dell'ePolicy affrontiamo tale problematica, con particolare

riferimento all'uso delle tecnologie digitali, e indichiamo le misure che la scuola intende attuare per garantire la tutela della privacy e il diritto alla riservatezza di tutti i soggetti coinvolti nel processo educativo, con particolare attenzione ai minori. A tal fine, l'Istituto allega alla presente ePolicy i modelli di liberatoria da utilizzare e conformi alla normativa vigente, in materia di protezione dei dati personali.

L'Istituto ospita alunni dai 3 ai 13 anni, per questo è fondamentale fare tutto il possibile per evitare che siano esposti a contenuti inappropriati.

In fase di iscrizione degli alunni alla scuola i genitori sottoscrivono un'informativa sul trattamento dei dati personali in ottemperanza all'art. 13 D.Lgs 30 giugno 2003 , n. 196 (Codice in materia di protezione dei dati personali).

All'inizio del ciclo di istruzione i genitori rilasciano il consenso all'utilizzo di materiale fotografico e audiovisivo riservato ed elaborati degli alunni per esporli anche in sedi diverse da quelle dell'Istituto quali pubblicazioni in formato digitale e siti web.

I dati sensibili sono ad esclusivo uso della dirigenza e della segreteria. I computer che contengono questi dati sono protetti da un ingresso con nome utente e password noti solo al personale preposto.

3.2 - Accesso ad Internet

1. *L'accesso a Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale.*
2. *Ogni persona ha eguale diritto di accedere a Internet in condizioni di parità, con modalità tecnologicamente adeguate e aggiornate che rimuovano ogni ostacolo di ordine economico e sociale.*
3. *Il diritto fondamentale di accesso a Internet deve essere assicurato nei suoi presupposti sostanziali e non solo come possibilità di collegamento alla Rete.*
4. *L'accesso comprende la libertà di scelta per quanto riguarda dispositivi, sistemi operativi e applicazioni anche distribuite.*
5. *Le Istituzioni pubbliche garantiscono i necessari interventi per il superamento di ogni forma di divario digitale tra cui quelli determinati dal genere, dalle condizioni economiche oltre che da situazioni di vulnerabilità personale e disabilità.*

Così recita l'art. 2 della Dichiarazione dei diritti di Internet, elaborata dalla Commissione per i diritti e i doveri in Internet, commissione costituita il 27 ottobre 2014 presso la Camera dei Deputati dalla presidente Laura Boldrini e presieduta da Stefano Rodotà. Inoltre, il 30 aprile 2016 era entrato in vigore il Regolamento UE del Parlamento Europeo e del Consiglio del 25 novembre 2015, che stabilisce le "misure

riguardanti l'accesso a un'Internet aperto e che modifica la direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica e il regolamento (UE) n. 531/2012 relativo al roaming sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione".

Il diritto di accesso a Internet è dunque presente nell'ordinamento italiano ed europeo e la scuola dovrebbe essere il luogo dove tale diritto è garantito, anche per quegli studenti che non dispongono della Rete a casa. In modo coerente il PNSD (Piano Nazionale Scuola Digitale) ha tra gli obiettivi quello di "fornire a tutte le scuole le condizioni per l'accesso alla società dell'informazione e fare in modo che il "diritto a Internet" diventi una realtà, a partire dalla scuola".

Questo perché le tecnologie da un lato contribuiscono a creare un ambiente che può rendere la scuola aperta, flessibile e inclusiva, dall'altro le consentono di adeguarsi ai cambiamenti della società e del mercato del lavoro, puntando a sviluppare una cultura digitale diffusa che deve iniziare proprio a scuola.

In ottemperanza all'art. 2 della Dichiarazione dei diritti di Internet, elaborata dalla Commissione per i diritti e i doveri in Internet, commissione costituita il 27 ottobre 2014 presso la Camera dei Deputati dalla presidente Laura Boldrini e presieduta da Stefano Rodotà. Inoltre, il 30 aprile 2016 era entrato in vigore il Regolamento UE del Parlamento Europeo e del Consiglio del 25 novembre 2015, che stabilisce le "misure riguardanti l'accesso a un'Internet aperto e che modifica la direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica e il regolamento (UE) n. 531/2012 relativo al roaming sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione".

Tutti i sei plessi d'Istituto sono dotati di accesso alla Rete Internet tramite wi-fi, rete protetta da password.

3.3 - Strumenti di comunicazione online

Le tecnologie digitali sono in grado di ridefinire gli ambienti di apprendimento, supportando la comunicazione a scuola e facilitando un approccio sempre più collaborativo. L'uso degli strumenti di comunicazione online a scuola, al fianco di quelli più tradizionali, ha l'obiettivo di rendere lo scambio comunicativo maggiormente interattivo e orizzontale. Tale uso segue obiettivi e regole precise correlati alle caratteristiche, funzionalità e potenzialità delle tecnologie digitali.

I pc dell'Istituto sono monitorati e tenuti aggiornati dai membri della Commissione

Innovazione Tecnologica che sono affiancati da tecnici esterni specializzati. In tre plessi è stato attivato un firewall per bloccare l'accesso a siti e contenuti inappropriati per il contesto scolastico.
La connessione alla rete wi-fi d'Istituto, riservata ai docenti per fini didattici, è accessibile solo in seguito ad inserimento di una password comune.
Tutte le aule sono dotate di pc portatili con accesso senza password, a disposizione dei docenti per la compilazione del registro elettronico e come supporto alla didattica.
I computer destinati ai ragazzi sono privi di password e vengono utilizzati sotto la supervisione di un insegnante.

3.4 - Strumentazione personale

I dispositivi tecnologici sono parte integrante della vita personale di ciascuno, compresa quella degli/lle studenti/esse e dei docenti (oltre che di tutte le figure professionali che a vario titolo sono inseriti nel mondo della scuola), ed influenzano necessariamente anche la didattica e gli stili di apprendimento. Comprendere il loro utilizzo e le loro potenzialità innovative, diventa di cruciale importanza, anche considerando il quadro di indirizzo normativo esistente e le azioni programmatiche, fra queste il Progetto Generazioni Connesse e il più ampio PNSD.

La presente ***ePolicy*** contiene indicazioni, revisioni o eventuali integrazioni di Regolamenti già esistenti che disciplinano l'uso dei dispositivi personali in classe, a seconda dei vari usi, anche in considerazione dei dieci punti del Miur per l'uso dei dispositivi mobili a scuola (BYOD, "Bring your own device").

Risulta fondamentale per la comunità scolastica aprire un dialogo su questa tematica e riflettere sulle possibilità per l'Istituto di dotarsi di una regolamentazione condivisa e specifica che tratti tali aspetti, considerando aspetti positivi ed eventuali criticità nella e per la didattica.

L'utilizzo di dispositivi personali è concesso al solo personale adulto presente nell'Istituto, i ragazzi possono utilizzarli all'inteno della scuola solo se espressamente richiesto dai docenti per specifiche attività didattiche.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2019/2020).

Scegliere almeno 1 di queste azioni:

- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali

AZIONI (da sviluppare nell'arco dei tre anni scolastici successivi).

- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

Capitolo 4 - Rischi on line: conoscere, prevenire e rilevare

4.1 - Sensibilizzazione e Prevenzione

Il rischio online si configura come la possibilità per il minore di:

- commettere azioni online che possano danneggiare se stessi o altri;
- essere una vittima di queste azioni;
- osservare altri commettere queste azioni.

È importante riconoscere questi fenomeni e saperli distinguere tra loro in modo da poter poi adottare le strategie migliori per arginarli e contenerli, ma è altrettanto importante sapere quali sono le possibili strategie da mettere in campo per ridurre la possibilità che questi fenomeni avvengano. Ciò è possibile lavorando su aspetti di ampio raggio che possano permettere una riduzione dei fattori di rischio e di conseguenza una minore probabilità che i ragazzi si trovino in situazioni non piacevoli. È importante che abbiano gli strumenti idonei per riconoscere possibili situazioni di rischio e segnalarle ad un adulto di riferimento.

Gli strumenti da adottare per poter ridurre l'incidenza di situazioni di rischio si configurano come interventi di **sensibilizzazione e prevenzione.**

- Nel caso della **sensibilizzazione** *si tratta di azioni che hanno come obiettivo quello di innescare e promuovere un cambiamento; l'intervento dovrebbe fornire non solo le informazioni necessarie (utili a conoscere il fenomeno), ma anche illustrare le possibili soluzioni o i comportamenti da adottare.*
- Nel caso della **prevenzione** *si tratta di un insieme di attività, azioni ed interventi attuati con il fine prioritario di promuovere le competenze digitali ed evitare l'insorgenza di rischi legati all'utilizzo del digitale e quindi ridurre i rischi per la sicurezza di bambine/i e ragazze/i.*

I docenti dell'Istituto si impegnano a formarsi e a far ricadere coinvolgere i ragazzi per avviarli verso le buone pratiche dell'uso consapevole della Rete e degli strumenti digitali.
I genitori si impegnano a prendere visione della E-safety Policy e a seguire le azioni promosse dalla scuola per l'utilizzo consapevole della rete.

Gli alunni si impegnano a rispettare i regolamenti e a partecipare attivamente alle occasioni di confronto su queste tematiche organizzate dalla scuola.
In presenza di appositi fondi la scuola si impegna altresì ad organizzare percorsi formativi su tematiche specifiche queli: grooming, cyberbullismo, furto di identità, sexting.

4.2 - Cyberbullismo: che cos'è e come prevenirlo

La legge 71/2017 "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo", nell'art. 1, comma 2, definisce il cyberbullismo:

"*qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo*".

La stessa legge e le relative **Linee di orientamento per la prevenzione e il contrasto del cyberbullismo** indicano al mondo scolastico ruoli, responsabilità e azioni utili a prevenire e gestire i casi di cyberbullismo. Le linee prevedono:

- formazione del personale scolastico, prevedendo la partecipazione di un proprio referente per ogni autonomia scolastica;
- sviluppo delle competenze digitali, tra gli obiettivi formativi prioritari (L.107/2015);
- promozione di un ruolo attivo degli studenti (ed ex studenti) in attività di peer education;
- previsione di misure di sostegno e rieducazione dei minori coinvolti;
- Integrazione dei regolamenti e del patto di corresponsabilità con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti;
- Il sistema scolastico deve prevedere azioni preventive ed educative e non solo sanzionatorie.
- **Nomina del Referente per le iniziative di prevenzione e contrasto che:**
    - Ha il compito di coordinare le iniziative di prevenzione e contrasto del cyberbullismo. A tal fine, può avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio.

- Potrà svolgere un importante compito di supporto al dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d'istituto), atti e documenti (PTOF, PdM, Rav).

Il cyberbullismo, come il bullismo tradizionale, è considerato un fenomeno di natura socio-relazionale che prevede un'asimmetria della relazione tra coetanei, ma si differenzia però per diversi elementi.
Le caratteristiche distintive del cyberbullismo sono:
a. l'anonimato reso possibile, ad esempio, attraverso l'utilizzo di uno pseudonimo;
b. l'assenza di relazione e di contatto diretto tra bullo e vittima. Nel bullo può contribuire a diminuire il livello di consapevolezza del danno arrecato e, d'altra parte, nella vittima, può rendere ancora più difficile sottrarsi alla prepotenza;
c. l'assenza di limiti spazio-temporali (motivo per cui l'elemento della "persistenza del tempo" che caratterizza il bullismo tradizionale assume qui valore e significati differenti).

Il Dirigente Scolastico ha individuato attraverso il Collegio dei Docenti un referente del bullismo e cyberbullismo al fine di coinvolge, prevenire e contrastare il fenomeno de bullismo, in tutte le componenti della comunità scolastica, ma in particolare quelle che operano nell'area dell'informatica.

Il Referente del "BULLISMO E CYBERBULLISMO":
- promuove la conoscenza e la consapevolezza del bullismo e del cyber-bullismo attraverso progetti
d'istituto che coinvolgano genitori, studenti e tutto il personale;
- coordina le attività di prevenzione ed informazione sulle sanzioni previste e sulle responsabilità di natura civile e penale, anche con eventuale affiancamento di genitori e studenti;
- si rivolge a partner esterni alla scuola, quali servizi sociali e sanitari, associazioni, aziende del privato sociale, forze di polizia, ecc., per realizzare un progetto di prevenzione;
- cura rapporti di rete fra scuole per eventuali convegni/seminari/corsi e per la giornata mondiale sulla Sicurezza in Internet la "Safer Internet Day".

Inoltre l'Istituto e il Refente del Bullismo e Cyberbullismo possono avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri specializzati del territorio.

4.3 - Hate speech: che cos'è e come prevenirlo

Il fenomeno di “incitamento all’odio” o “discorso d’odio”, indica discorsi (post, immagini, commenti etc.) e pratiche (non solo online) che esprimono odio e intolleranza verso un gruppo o una persona (identificate come appartenente a un gruppo o categoria) e che rischiano di provocare reazioni violente, a catena. Più ampiamente il termine “hate speech” indica un’offesa fondata su una qualsiasi discriminazione (razziale, etnica, religiosa, di genere o di orientamento sessuale, di disabilità, eccetera) ai danni di una persona o di un gruppo.

Tale fenomeno, purtroppo, è sempre più diffuso ed estremamente importante affrontarlo anche a livello educativo e scolastico con l’obiettivo di:

- fornire agli studenti gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di hate speech, in particolare legati alla razza, al genere, all’orientamento sessuale, alla disabilità;
- promuovere la partecipazione civica e l’impegno, anche attraverso i media digitali e i social network;
- favorire una presa di parola consapevole e costruttiva da parte dei giovani.

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere in relazione a questa problematica.

Il fenomeno di “incitamento all’odio” o “discorso d’odio”, nelle diverse forme: post, immagini, commenti etc. e pratiche, non solo online che esprimono odio e intolleranza verso un gruppo o una persona e che rischiano di provocare reazioni violente, a catena sono in aumento. Allo stesso modo avviene con l'“hate speech” che indica un’offesa fondata su una qualsiasi discriminazione: razziale, etnica, religiosa, di genere o di orientamento sessuale, di disabilità, eccetera ai danni di una persona o di un gruppo. Per questo la scuola è chiamata a far riflettere i ragazzi su queste problematiche.

Per affrontare questi temi l'Istituto ha deciso di porre attenzione allo sviluppo delle competenze digitali e l’educazione ad un uso etico e consapevole delle tecnologie assumendo quindi un ruolo centrale anche per la promozione della consapevolezza di queste dinamiche in rete. Occorre, in tal senso, valorizzare la dimensione relazionale e fornire ai più giovani gli strumenti necessari per eliminare gli stereotipi su cui spesso si fondano forme di hate speech, in particolare legati alla razza, al genere, all’orientamento sessuale, alla disabilità.

In presenza di appositi fondi la scuola si impegna altresì ad organizzare percorsi formativi su tematiche specifiche si potrà avvalere di consulenti/esperti esterni per organizzare incontri formativi rivolti a docenti, genitori ed alunni.

4.4 - Dipendenza da Internet e gioco

online

La Dipendenza da Internet fa riferimento all'utilizzo eccessivo e incontrollato di Internet che, al pari di altri comportamenti patologici/dipendenze, può causare o essere associato a isolamento sociale, sintomi da astinenza, problematiche a livello scolastico e irrefrenabile voglia di utilizzo della Rete.

L'istituto è intenzionato a promuovere azioni di prevenzione attraverso percorsi sul benessere digitale?

La Dipendenza da Internet fa riferimento all'utilizzo eccessivo e incontrollato di Internet che, al pari di altri comportamenti patologici/dipendenze, può causare o essere associato a isolamento sociale, sintomi da astinenza, problematiche a livello scolastico e irrefrenabile voglia di utilizzo della Rete. L'istituto propone da anni incontri con esperti per affrontare il variegato mondo delle dipendenze. Vista la giovane età dei fruitori della rete, si cerca di sensibilizzare le famiglie a monitorare le ore trascorse online. I Docenti e gli esperti cercano di far comprendere ai ragzzi la differenza tra "momento" di gioco di svago e "necesasità" di gioacere in rete.

4.5 - Sexting

Il "sexting" è fra i rischi più diffusi connessi ad un uso poco consapevole della Rete. Il termine indica un fenomeno molto frequente fra i giovanissimi che consiste nello scambio di contenuti mediali sessualmente espliciti; i/le ragazzi/e lo fanno senza essere realmente consapevoli di scambiare materiale (pedopornografico) che potrebbe arrivare in mani sbagliate e avere conseguenze impattanti emotivamente per i protagonisti delle immagini, delle foto e dei video.

Il "sexting" è fra i rischi più diffusi connessi ad un uso poco consapevole della Rete. Il termine indica un fenomeno molto frequente fra i giovanissimi che consiste nello scambio di contenuti mediali sessualmente espliciti; i/le ragazzi/e lo fanno senza essere realmente consapevoli di scambiare materiale (pedopornografico) che potrebbe arrivare in mani sbagliate e avere conseguenze impattanti emotivamente per i protagonisti delle immagini, delle foto e dei video.

L'Istituto ritiene che per prevenire il "sexting" sia necessario svolgere un percorso specifico. Per quasto propone nei vari anni di scuola un percorso formativo che ha come finalità la prevenzione della devianza e del disagio giovanile che permetta la costruzione dello "star bene" con sé e con gli altri.

L'Istituto organizza attività, progetti, corsi, eventi con l'obiettivo di coinvolgere, informare genitori, insegnanti e, in generale, gli adulti educatori sulle tematiche inerenti la formazione dei ragazzi sui seguenti temi:

- Alfabetizzazione emotiva
- Autostima
- Socializzazione e dinamiche relazionali
- Cooperazione
- Educazione sessuale e relazionale-affettiva.

4.6 - Adescamento online

Il ***grooming*** (dall'inglese "groom" - curare, prendersi cura) rappresenta una tecnica di manipolazione psicologica che gli adulti potenziali abusanti utilizzano per indurre i bambini/e o adolescenti a superare le resistenze emotive e instaurare una relazione intima e/o sessualizzata. Gli adulti interessati sessualmente a bambini/e e adolescenti utilizzano spesso anche gli strumenti messi a disposizione dalla Rete per entrare in contatto con loro.

I luoghi virtuali in cui si sviluppano più frequentemente tali dinamiche sono le chat, anche quelle interne ai giochi online, i social network in generale, le varie app di instant messaging (whatsapp, telegram etc.), i siti e le app di ***teen dating*** (siti di incontri per adolescenti). Un'eventuale relazione sessuale può avvenire, invece, attraverso webcam o live streaming e portare anche ad incontri dal vivo. In questi casi si parla di adescamento o grooming online.

In Italia l'adescamento si configura come reato dal 2012 (art. 609-undecies – l'adescamento di minorenni) quando è stata ratificata la Convenzione di Lanzarote (legge 172 del 1° ottobre 2012).

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere per prevenire ed affrontare la delicata problematica dell'adescamento.

Il grooming (dall'inglese "groom" - curare, prendersi cura) rappresenta una tecnica di manipolazione psicologica che gli adulti potenziali abusanti utilizzano per indurre i bambini/e o adolescenti a superare le resistenze emotive e instaurare una relazione intima e/o sessualizzata. Gli adulti interessati sessualmente a bambini/e e adolescenti utilizzano spesso anche gli strumenti messi a disposizione dalla Rete per entrare in contatto con loro.

L'Istituto ritiene che per prevenire il "grooming" sia necessario svolgere un percorso specifico. Per quasto propone nei vari anni di scuola un percorso formativo che ha

come finalità la prevenzione della devianza e del disagio giovanile che permetta la costruzione dello “star bene” con sé e con gli altri.
L'Istituto organizza attività, progetti, corsi, eventi con l’obiettivo di coinvolgere, informare genitori, insegnanti e, in generale, gli adulti educatori sulle tematiche inerenti la formazione dei ragazzi sui seguenti temi:

- Alfabetizzazione emotiva
- Autostima
- Socializzazione e dinamiche relazionali
- Cooperazione
- Educazione sessuale e relazionale-affettiva.

4.7 - Pedopornografia

La pedopornografia online è un reato (art. 600-ter comma 3 del c.p.) che consiste nel produrre, divulgare, diffondere e pubblicizzare, anche per via telematica, immagini o video ritraenti bambini/e, ragazzi/e coinvolti/e in comportamenti sessualmente espliciti, **concrete o simulate** o qualsiasi rappresentazione degli organi sessuali a fini soprattutto sessuali.

La legge n. 269 del 3 agosto 1998 *“Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di schiavitù”, introduce nuove fattispecie di reato (come ad esempio il turismo sessuale) e, insieme alle successive modifiche e integrazioni contenute nella* ***legge n. 38 del 6 febbraio 2006*** *“Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet”*, segna una tappa fondamentale nella definizione e predisposizione di strumenti utili a contrastare i fenomeni di sfruttamento sessuale a danno di minori. Quest’ultima, introduce, tra le altre cose, il reato di “pornografia minorile virtuale” (artt. 600 ter e 600 quater c.p.) che si verifica quando il materiale pedopornografico rappresenta immagini relative a bambini/e ed adolescenti, realizzate con tecniche di elaborazione grafica non associate, in tutto o in parte, a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali.

Secondo la Legge 172/2012 - *Ratifica della Convenzione di Lanzarote (Art 4.) per pornografia minorile si intende ogni rappresentazione, con qualunque mezzo, di un minore degli anni diciotto coinvolto in attività sessuali esplicite, reali o simulate, o qualunque rappresentazione degli organi sessuali di un minore di anni diciotto per scopi sessuali.*

In un’ottica di attività preventive, il tema della pedopornografia è estremamente delicato, occorre parlarne sempre in considerazione della maturità, della fascia d’età e

selezionando il tipo di informazioni che si possono condividere.

La pedopornografia è tuttavia un fenomeno di cui si deve sapere di più, ed è utile parlarne, in particolare se si vogliono chiarire alcuni aspetti legati alle conseguenze impreviste del sexting.

Inoltre, è auspicabile che possa rientrare nei temi di un'attività di sensibilizzazione rivolta ai genitori e al personale scolastico promuovendo i servizi di Generazioni Connesse: qualora navigando in Rete si incontri materiale pedopornografico è opportuno segnalarlo, anche anonimamente, attraverso il sito www.generazioniconnesse.it alla sezione **"Segnala contenuti illegali"** (Hotline).

Il servizio Hotline si occupa di raccogliere e dare corso a segnalazioni, inoltrate anche in forma anonima, relative a contenuti pedopornografici e altri contenuti illegali/dannosi diffusi attraverso la Rete. I due servizi messi a disposizione dal Safer Internet Centre sono il "Clicca e Segnala" di Telefono Azzurro e "STOP-IT" di Save the Children.

La pedopornografia online è un reato che consiste nel produrre, divulgare, diffondere e pubblicizzare, anche per via telematica, immagini o video ritraenti bambini/e, ragazzi/e coinvolti/e in comportamenti sessualmente espliciti, concrete o simulate o qualsiasi rappresentazione degli organi sessuali a fini soprattutto sessuali.

L'Istituto ritiene che per prevenire il fenomeno della "pedopornografia" sia necessario svolgere un percorso specifico. Per quasto propone nei vari anni di scuola un percorso formativo che ha come finalità la prevenzione della devianza e del disagio giovanile che permetta la costruzione dello "star bene" con sé e con gli altri.
L'Istituto organizza attività, progetti, corsi, eventi con l'obiettivo di coinvolgere, informare genitori, insegnanti e, in generale, gli adulti educatori sulle tematiche inerenti la formazione dei ragazzi sui seguenti temi:

- Alfabetizzazione emotiva
- Autostima
- Socializzazione e dinamiche relazionali
- Cooperazione
- Educazione sessuale e relazionale-affettiva.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2019/2020).

☐ Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli

studenti/studentesse.

AZIONI (da sviluppare nell’arco dei tre anni scolastici successivi).

□ Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all’utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti.

Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

Il personale docente del nostro Istituto quando ha il sospetto o la certezza che uno/a studente/essa possa essere vittima o responsabile di una situazione di cyberbullismo, sexting o adescamento online ha a disposizione procedure definite e può fare riferimento a tutta la comunità scolastica.

Questa sezione dell'ePolicy contiene le procedure standardizzate per la segnalazione e gestione dei problemi connessi a comportamenti online a rischio di studenti e studentesse (vedi allegati a seguire).

Tali procedure dovranno essere una guida costante per il personale della scuola nell'identificazione di una situazione online a rischio, così da definire le modalità di presa in carico da parte della scuola e l'intervento migliore da mettere in atto per aiutare studenti/esse in difficoltà. Esse, inoltre, forniscono valide indicazioni anche per i professionisti e le organizzazioni esterne che operano con la scuola (vedi paragrafo 1.3. dell'ePolicy).

Nelle procedure:

- sono indicate le **figure preposte all'accoglienza della segnalazione e alla presa in carico e gestione del caso**.
- le modalità di coinvolgimento del referente per il contrasto del bullismo e del cyberbullismo, oltre al Dirigente Scolastico.

Inoltre, la scuola **individua le figure che costituiranno un team** preposto alla gestione della segnalazione (gestione interna alla scuola, invio ai soggetti competenti).

Nell'affrontare i casi prevediamo la **collaborazione con altre figure, enti, istituzioni e servizi presenti sul territorio** (che verranno richiamati più avanti), qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.

Tali procedure sono comunicate e condivise con l'intera comunità scolastica.

Questo risulta importante sia per facilitare l'emersione di situazioni a rischio, e la conseguente presa in carico e gestione, sia per dare un messaggio chiaro a studenti e

studentesse, alle famiglie e a tutti coloro che vivono la scuola che la stessa è un luogo sicuro, attento al benessere di chi lo vive, in cui le problematiche non vengono ignorate ma gestite con una mobilitazione attenta di tutta la comunità.

La condivisione avverrà attraverso assemblee scolastiche che coinvolgono i genitori, gli studenti e le studentesse e il personale della scuola, con l'utilizzo di locandine da affiggere a scuola, attraverso news nel sito della scuola e durante i collegi docenti e attraverso tutti i canali maggiormente utili ad un'efficace comunicazione.

A seguire, le problematiche a cui fanno riferimento le procedure allegate:

- **Cyberbullismo**: è necessario capire se si tratta effettivamente di cyberbullismo o di altra problematica. Oltre al contesto, vanno considerate le modalità attraverso le quali il comportamento si manifesta (alla presenza di un "pubblico"? Tra coetanei? In modo ripetuto e intenzionale? C'è un danno percepito alla vittima? etc.). È necessario poi valutare l'eventuale stato di disagio vissuto dagli/lle studenti/esse coinvolti/e (e quindi valutare se rivolgersi ad un servizio deputato ad offrire un supporto psicologico e/o di mediazione).
- **Adescamento online**: se si sospetta un caso di adescamento online è opportuno, innanzitutto, fare attenzione a non cancellare eventuali prove da smartphone, tablet e computer utilizzati dalla persona minorenne e inoltre è importante non sostituirsi al bambino/a e/o adolescente, evitando, quindi, di rispondere all'adescatore al suo posto). È fondamentale valutare il benessere psicofisico dei minori e il rischio che corrono. Vi ricordiamo che l'attuale normativa prevede che la persona coinvolta in qualità di vittima o testimone in alcune tipologie di reati, tra cui il grooming, debba essere ascoltata in sede di raccolta di informazioni con l'ausilio di una persona esperta in psicologia o psichiatria infantile.
- **Sexting**: nel caso in cui immagini e/o video, anche prodotte autonomamente da persone minorenni, sfuggano al loro controllo e vengano diffuse senza il loro consenso è opportuno adottare sistemi di segnalazione con l'obiettivo primario di tutelare il minore e ottenere la rimozione del materiale, per quanto possibile, se online e il blocco della sua diffusione via dispositivi mobili.

Per quanto riguarda la necessità di segnalazione e rimozione di contenuti online lesivi, ciascun minore ultraquattordicenne (o i suoi genitori o chi esercita la responsabilità del minore) che sia stato vittima di cyberbullismo può inoltrare al titolare del trattamento o al gestore del sito internet o del social media un'istanza per l'oscuramento, la rimozione o il blocco dei contenuti diffusi nella Rete. Se entro 24 ore il gestore non avrà provveduto, l'interessato può rivolgere analoga richiesta al Garante per la protezione dei dati personali, che rimuoverà i contenuti entro 48 ore.

Vi suggeriamo, inoltre, i seguenti servizi:

- Servizio di Helpline 19696 e Chat di Telefono Azzurro per supporto ed emergenze;

- Clicca e segnala di Telefono Azzurro e STOP-IT di Save the Children Italia per

segnalare la presenza di materiale pedopornografico online.

Il personale docente del nostro Istituto quando ha il sospetto o la certezza che uno/a studente/essa possa essere vittima o responsabile di una situazione di bullismo o cyberbullismo, sexting o adescamento online . In particolare è tenuto a segnaaere casi in cui viene a conoscenza dei seguenti fatti:

Violenza fisica, psicologica o l'intimidazione del gruppo, specie se reiterata;
Flaming: litigi on line nei quali si fa uso di un linguaggio violento e volgare.
Harassment: molestie attuate attraverso l'invio ripetuto di linguaggi offensivi.
Cyberstalking: invio ripetuto di messaggi che includono esplicite minacce fisiche, al punto che la vittima arriva a temere per la propria incolumità.
Denigrazione: pubblicazione all'interno di comunità virtuali, quali newsgroup, blog, forum di discussione, messaggistica immediata, siti Internet, ecc., di pettegolezzi e commenti crudeli, calunniosi e denigratori.
Outing estorto: registrazione delle confidenze – raccolte all'interno di un ambiente privato - creando un clima di fiducia e poi inserite integralmente in un blog pubblico.
Impersonificazione: insinuazione all'interno dell'account di un'altra persona con l'obiettivo di inviare dal medesimo messaggi ingiuriosi che screditino la vittima.
Esclusione: estromissione intenzionale dall'attività on line.
Sexting: invio di messaggi via smartphone ed Internet, corredati da immagini a sfondo sessuale

---

5.2. - Come segnalare: quali strumenti e a chi

L'insegnante riveste la qualifica di pubblico ufficiale in quanto l'esercizio delle sue funzioni non è circoscritto all'ambito dell'apprendimento, ossia alla sola preparazione e tenuta delle lezioni, alla verifica/valutazione dei contenuti appresi dagli studenti e dalle studentesse, ma si estende a tutte le altre attività educative.

Le situazioni problematiche in relazione all'uso delle tecnologie digitali dovrebbero essere sempre gestite anche a livello di gruppo.

Come descritto nelle procedure di questa sezione, si potrebbero palesare due casi:

- CASO A (SOSPETTO) – Il docente ha il sospetto che stia avvenendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.
- CASO B (EVIDENZA) – Il docente ha evidenza certa che stia accadendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di

bullismo e/o cyberbullismo, sexting o adescamento online.

Per tutti i dettagli fate riferimento agli allegati con le procedure.

Strumenti a disposizione di studenti/esse

Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione:

- un indirizzo e-mail specifico per le segnalazioni;
- scatola/box per la raccolta di segnalazioni anonime da inserire in uno spazio accessibile e ben visibile della scuola;
- sportello di ascolto con professionisti;
- docente referente per le segnalazioni.

Anche studenti e studentesse, inoltre, possono rivolgersi alla Helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

All'interno della procedura disciplinare, che vale per qualsiasi comportamento contrario al regolamento di Istituto, si inserisce una parte specifica per gli episodi di bullismo e cyberbullismo in base all'attuale normativa:

- attraverso la compilazione del modulo in formato cartaceo opportunamente predisposto, viene effettuata una segnalazione al referente per il bullismo ed il cyberbullismo che ne dà immediata comunicazione al Dirigente Scolatico il quale valuta se ricorrono gli estremi per una denuncia;
la segnalazione può essere anonima, ma va sempre riportata per iscritto anche se raccolta oralmente.

Nel caso in cui la segnalazione arrivi direttamente al Dirigente Scolatico, questi procederà come da prescrizioni normative:
- il fatto non costituisce reato o ipotizza un reato a querela di parte: il Dirigente Scolatico. informa tempestivamente i soggetti esercenti la responsabilità genitoriale, ovvero i tutori dei minori coinvolti e attiva adeguate azioni di carattere educativo;
- il D.S. ha notizia di reato: sporge subito denuncia per iscritto all'autorità giudiziaria (Questura, Carabinieri, ecc.), anche quando non sia individuata la persona alla quale il reato è attribuito (art 331 cpp);
- si evidenzia che sia la detenzione che la divulgazione di qualsiasi immagine di tipo

sessuale o di esposizione di nudità (prodotto anche attraverso la pratica del "sexting") è considerato dalla legislazione vigente materiale pedopornografico; è, pertanto, necessario comunicarlo immediatamente al Dirigente Scolatico perché trasmetta la notizia tempestivamente, con relazione circostanziata, alla polizia postale o altra forza di polizia;
- quando un docente o un componente del personale A.T.A. viene a conoscenza di un comportamento ipotizzabile verosimilmente e ragionevolmente come reato ha l'obbligo di comunicarlo con la massima urgenza al Dirigente Scolatico perché adotti le misure necessarie.

5.3. - Gli attori sul territorio

Talvolta, nella gestione dei casi, può essere necessario rivolgersi **ad altre figure, enti, istituzioni e servizi presenti sul territorio** qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.

Per una mappatura degli indirizzi di tali strutture è possibile consultare il Vademecum di Generazioni Connesse "Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all'utilizzo delle tecnologie digitali da parte dei più giovani" (seconda parte, pag. 31), senza dimenticare che la Helpline di Telefono Azzurro (19696) è sempre attiva nell'offrire una guida competente ed un supporto in tale percorso.

A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all'utilizzo di Internet può presentare.

- **Comitato Regionale Unicef**: laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni)**: svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare attenzione alla tutela dei minori.
- **Ufficio Scolastico Regionale**: supporta le scuole in attività di prevenzione ed anche nella segnalazione di comportamenti a rischio correlati all'uso di Internet.
- **Polizia Postale e delle Comunicazioni**: accoglie tutte le segnalazioni relative a comportamenti a rischio nell'utilizzo della Rete e che includono gli estremi del reato.
- **Aziende Sanitarie Locali**: forniscono supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in Rete. In

alcune regioni, come il Lazio e la Lombardia, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da Internet e alle situazioni di rischio correlate.

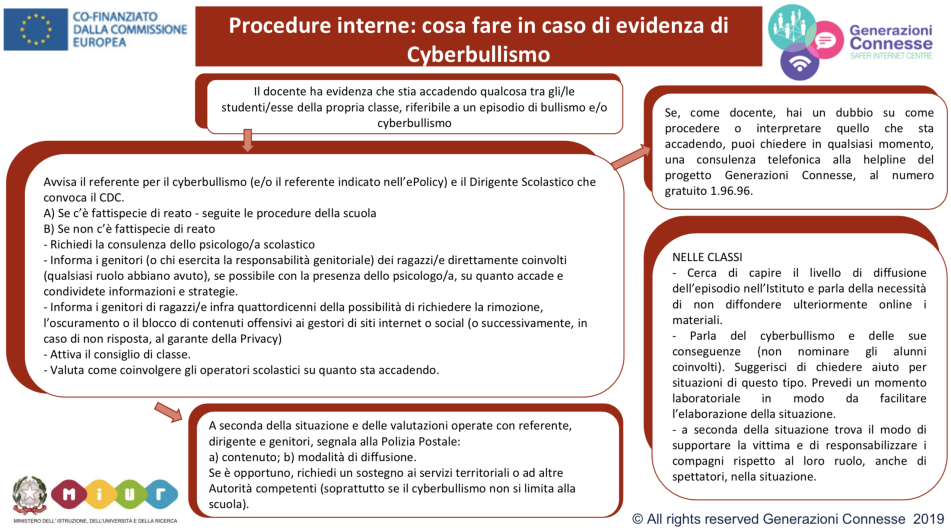
- **Garante Regionale per l'Infanzia e l'Adolescenza e Difensore Civico**: segnalano all'Autorità Giudiziaria e ai Servizi Sociali competenti; accolgono le segnalazioni di presunti abusi e forniscono informazioni sulle modalità di tutela e di esercizio dei diritti dei minori vittime. Segnalano alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.
- **Tribunale per i Minorenni**: segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

Nella gestione dei casi, può essere necessario rivolgersi ad altre figure, enti, istituzioni e servizi presenti sul territorio qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.

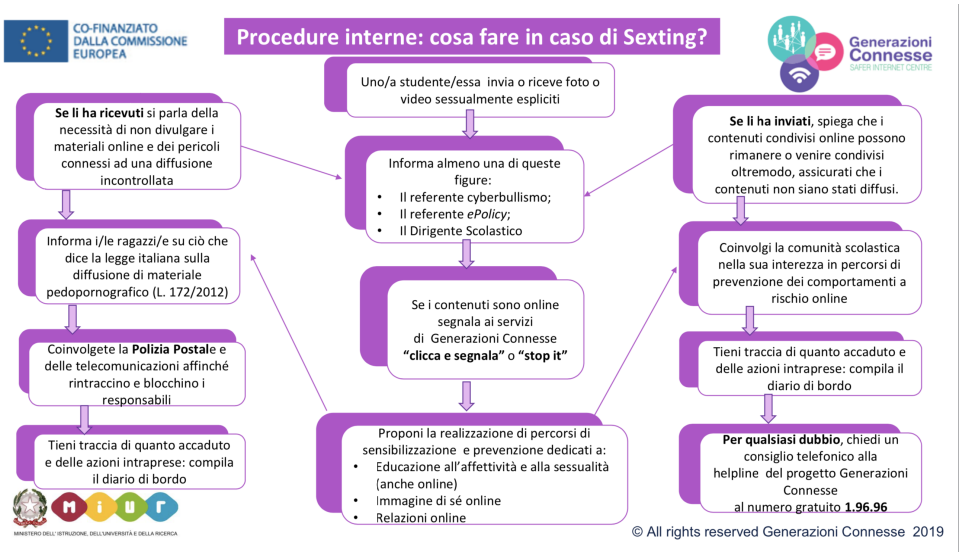
Ufficio Scolastico Regionale: supporta le scuole in attività di prevenzione ed anche nella segnalazione di comportamenti a rischio correlati all'uso di Internet.
Polizia Postale e delle Comunicazioni: accoglie tutte le segnalazioni relative a comportamenti a rischio nell'utilizzo della Rete e che includono gli estremi del reato.
Aziende Sanitarie Locali: forniscono supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in Rete. In Lombardia, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da Internet e alle situazioni di rischio correlate.
Garante Regionale per l'Infanzia e l'Adolescenza e Difensore Civico: segnalano all'Autorità Giudiziaria e ai Servizi Sociali competenti; accolgono le segnalazioni di presunti abusi e forniscono informazioni sulle modalità di tutela e di esercizio dei diritti dei minori vittime. Segnalano alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.
Tribunale per i Minorenni: segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

5.4. - Allegati con le procedure

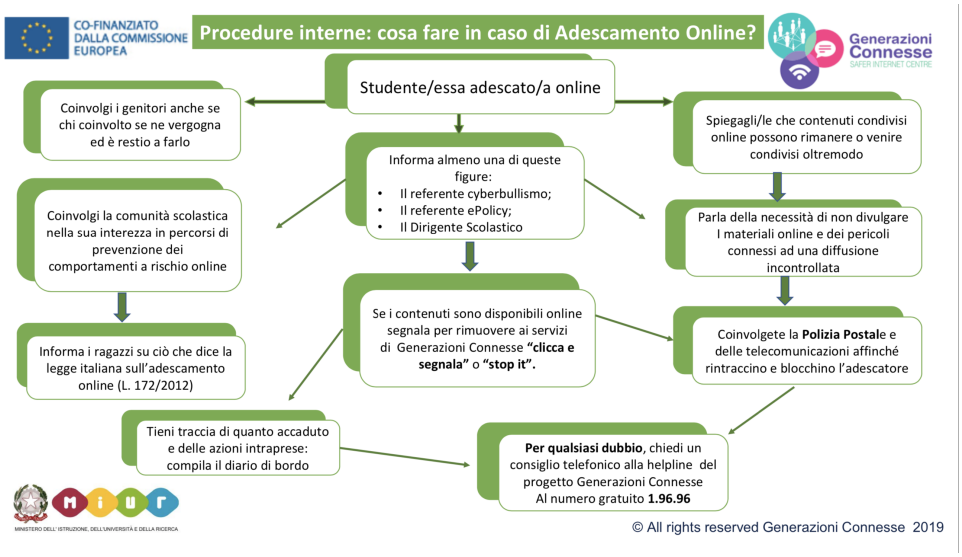
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



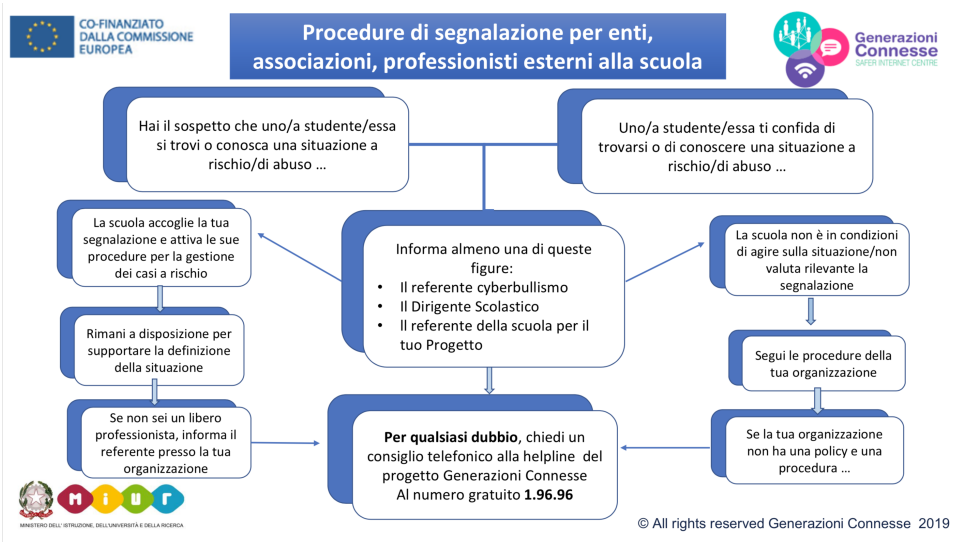
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



Procedure di segnalazione per enti, associazioni, professionisti esterni alla scuola



Altri allegati

- Scheda di segnalazione
- Diario di bordo
- iGloss@ 1.0 l'ABC dei comportamenti devianti online
- Elenco reati procedibili d'ufficio

elenco reati procedibili d'ufficio

l'ABC dei comportamenti devianti online

diario di bordo

scheda di segnalazione

1-Procedura di segnalazione interna - cyberbullismo

2-Procedura di segnalazione interna - sexting

3-Procedura di segnalazione interna - adescamento

4-Procedura di segnalazione enti esterni

Il nostro piano d'azioni

Non è prevista nessuna azione.