Sintesi Documento ePolicy

TOIC865006

I.C. FAVRIA

PIAZZA REPUBBLICA 6 - 10083 - FAVRIA - TORINO (TO)

Valeria Miotti

Capitolo 1 - Introduzione al documento di ePolicy

Scopo dell'ePolicy

L'E-policy è 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.

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.

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.

Disciplina degli alunni

Le infrazioni in cui è possibile che gli alunni incorrano a scuola nell'utilizzo delle tecnologie digitali , in relazione alla fascia di età considerate, sono prevedibilmente le seguenti :

- uso inappropriato della Rete;
- un uso della rete per giudicare , infastidire o impedire a qualcuno di esprimersi o partecipare;
- l'invio incauto o senza permesso di foto o di altri dati personali come l'indirizzo di casa o il telefono;
- la condivisione di immagini intime o inadeguate;

- la comunicazione incauta e senza permesso con sconosciuti

Gli interventi correttivi sono rapportati all'età e al livello di sviluppo del bambino.
Sono previsti pertanto, da parte dei docenti, provvedimenti disciplinari proporzionati all'età e alla gravità del comportamento , quali:

- il richiamo verbale;
- il richiamo scritto con annotazione sul diario e sul Registro elettronico;
- la convocazione dei genitori da parte degli insegnanti;
- la convocazione dei genitori da parte del Ds;
- l'eventuale provvedimento disciplinare deciso dal consiglio di classe o interclasse

Contestualmente sono previsti interventi di carattere educativo di rinforzo dei comportamenti corretti e riparativi dei disagi causati, di ri-definizione delle regole sociali di convivenza attraverso la partecipazione consapevole e attiva degli alunni della classe, di prevenzione e gestione positiva dei conflitti, di moderazione dell'eccessiva competitività, di promozione di rapporti amicali e di reti di solidarietà, di promozione della conoscenza e della gestione delle emozioni.

Disciplina del personale scolastico

Le potenziali infrazioni, in cui è possibile che il personale scolastico e in particolare i docenti incorrano nell'utilizzo delle tecnologie digitali e di internet, sono diverse e alcune possono determinare , favorire o avere conseguenze di maggiore o minore rilievo sull'uso corretto e responsabile delle TIC da parte degli alunni :

- un utilizzo delle tecnologie e dei servizi della scuola , d'uso comune con gli alunni , non connesso alle attività di insegnamento o al profilo professionale, anche tramite l'installazione di software o il salvataggio di materiali non idonei ;
- un utilizzo delle comunicazioni elettroniche con i genitori e gli alunni non compatibile con il ruolo professionale;
- un trattamento dei dati personali, comuni e sensibili degli alunni, non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi ;
- una diffusione delle password assegnate e una custodia non adeguata degli strumenti e degli accessi di cui possono approfittare terzi;
- una carente istruzione preventiva degli alunni sull'utilizzazione corretta e responsabile delle tecnologie digitali e di internet;
- una vigilanza elusa degli alunni che può favorire un utilizzo non autorizzato delle TIC e possibili incidenti;
- insufficienti interventi nelle situazioni critiche di contrasto a terzi , correttivi o di sostegno agli alunni, di segnalazioni ai genitori , al Dirigente scolastico o all'Animatore digitale .

Il Dirigente Scolastico può controllare l'utilizzo delle TIC per verificarne la conformità alle regole di sicurezza, compreso l'accesso a internet, la posta elettronica inviata/pervenuta a scuola, procedere alla cancellazione di materiali inadeguati o non autorizzati dal sistema informatico della scuola, conservandone copia per eventuali successive investigazioni.
Tutto il personale è tenuto a collaborare con il Ds e a fornire ogni informazione utile per le valutazioni del caso e per l'avvio di procedimenti che possono avere carattere organizzativo, gestionale , disciplinare , amministrativo, penale a seconda del tipo o della gravità delle infrazioni commesse . Le procedure sono quelle previste dalla legge e dai contratti di lavoro.

Disciplina dei genitori

In considerazione dell'età dei bambini (fino a 14 anni) e della loro dipendenza dagli adulti, alcune considerazioni e condotte dei genitori possono favorire o meno l'uso corretto e responsabile delle TIC da parte degli alunni a scuola, luogo in cui possono portare materiali e strumenti o comunicare problematiche sorte al di fuori del contesto scolastico.
Le situazioni familiari meno favorevoli sono:

- la convinzione che se il proprio figlio rimane a casa ad usare il computer è al sicuro e non combinerà guai;
- una piena autonomia concessa al proprio figlio nella navigazione sul web e nell'utilizzo del cellulare o dello smartphone;
- un utilizzo del pc, del cellulare o dello smartphone in comune con gli adulti che possono conservare in memoria materiali non idonei

I genitori degli alunni possono essere convocati a scuola per concordare misure educative diverse oppure essere sanzionabili a norma di legge in base alla gravità dei comportamenti dei loro figli, se dovessero risultare pericolosi per sé e/o dannosi per altri, in relazione soprattutto a materiale o situazioni che abbiano ripercussione in ambito scolastico.

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.

Verranno inserite le seguenti norme:

1.DIVIETI

E' vietato installare materiale protetto da copyright. E' vietato l'uso della postazione di lavoro per i collegamenti a Internet a scopi commerciali o di profitto personale o di attività illegali. Ricordando che la responsabilità delle azioni compiute tramite una utenza è sempre del legittimo titolare , anche se compiute in sua assenza , la password ricevuta non deve essere comunicata a nessuno e non deve essere salvata su dispositivi di uso comune . Essa deve essere memorizzata dall'utente che non deve trascriverla in nessun luogo . Ogni contatto ed operazione on line che implica assunzione di impegni o responsabilità per conto della scuola deve essere autorizzata dal legale rappresentante dell'istituzione.

2.USO PERSONALE

E' consentito l'utilizzo della postazione di lavoro , in modo saltuario , a fini personali , solo se compatibile o funzionale al ruolo professionale svolto purchè non sia causa diretta o indiretta, di disservizi dei sistemi elaborativi e dei servizi di collegamento dell'Amministrazione ; non sia causa di oneri aggiuntivi per l'Amministrazione , non interferisca con le attività lavorative dell'utente , delle attività scolastiche o con altri obblighi dello stesso verso l'Amministrazione .

3.USO DIDATTICO

- Ogni allievo è direttamente responsabile della postazione assegnatagli per le ore in cui vi svolge lezione . Agli utenti è fatto assoluto divieto di cancellare ,modificare in qualsiasi modo i files presenti sulla macchina o alterare il sistema operativo o la configurazione dei programmi e dell'hardware della macchina .
- E' fatto obbligo di adottare comportamenti idonei a non provocare danni o pericoli agli strumenti ed alle attrezzature messi a disposizione . In caso di comodato d'uso dei device di proprietà o in concessione all'Istituto si fa riferimento al contratto.
- Gli utenti sono tenuti a non prelevare o depositare informazioni, applicazioni o documenti che possano in qualsiasi modo arrecare danno a persone , cose o istituzioni
- E' vietato inserire file sul server o scaricare da internet software non autorizzati o materiale soggetto a copyright o a diritti di proprietà intellettuale.
- Il riscontro di qualsiasi anomalia deve essere tempestivamente segnalato dagli alunni al docente e dal docente al responsabile del laboratorio.
- Per utilizzare CD-ROM , DVD , penne USB o altri supporti di memorizzazione personali è necessario sottoporli al controllo anti virus.
- Si devono rispettare le regole di decenza e morali, evitare atti e comportamenti che possano recare offesa a cose , persone o istituzioni presenti o meno sulla rete.
- E' fatto assoluto divieto di navigare in siti dai contenuti pornografici o contenenti scene di violenza , razzismo o sfruttamento dei minori.
- Si deve mantenere segreto il nome, l'indirizzo, il telefono di casa, il telefono cellulare , il nome e l'indirizzo della scuola frequentata.
- Non si devono inviare a nessuno fotografie proprie o di amici

I docenti che accompagnano gli allievi in laboratorio o fanno usare i dispositivi di classe o i loro dispositivi (vedasi BYOD) sono tenuti a controllare che vengano rispettati i divieti sopraelencati e che l'utilizzo delle risorse tecnologiche sia finalizzato agli intenti didattici previsti .

Capitolo 2 - Formazione e curricolo

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.

Traguardi per lo sviluppo delle competenze digitali al termine della SCUOLA DELL'INFANZIA

L'alunno:

- sperimenta situazioni problematiche sviluppando le basi del pensiero computazionale;
- esperisce attività di coding unplugged collegando trasversalmente i vari campi d'esperienza;

Traguardi per lo sviluppo delle competenze digitali al termine della SCUOLA PRIMARIA

L'alunno:

- utilizza le più comuni tecnologie in particolare quelle dell'informazione e della comunicazione individuando le soluzioni potenzialmente utili ad un dato contesto applicativo, a partire dall' attività di studi fino alla risoluzione di problemi della vita quotidiana;
- è consapevole delle potenzialità, dei limiti e dei rischi dell'uso delle tecnologie, con particolare riferimento al contesto produttivo, culturale e sociale in cui vengono applicate;
- cerca, utilizza e crea in modo critico le informazioni condivise in Rete, valutandone credibilità e affidabilità;
- gestisce in modo sicuro i propri dati personali e quelli altrui e utilizza le tecnologie digitali per scopi eticamente accettabili, nel rispetto degli altri.

Traguardi per lo sviluppo delle competenze digitali al termine della SCUOLA SECONDARIA I GRADO

L'alunno:

- reperisce, seleziona e valuta informazioni in internet da fonti e con strumenti diversi;
- utilizza in modo etico gli strumenti per comunicare ed evitare le possibili minacce alla privacy e altri reati in rete;
- ha buone competenze digitali, usa con consapevolezza le tecnologie della comunicazione per ricercare e analizzare dati e saper distinguere informazioni attendibili da quelle che necessitano approfondimento;
- è in grado di usare, in modo efficace e responsabile, le nuove tecnologie e i linguaggi multimediali per supportare lo studio e il lavoro progettuale, sia a livello individuale che collaborando e cooperando con i compagni;
- sviluppa particolari abilità socio-comunicative e partecipative per maturare una maggiore consapevolezza sui doveri nei riguardi di coloro con cui si comunica online.

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

Protezione dei dati personali, accesso ad Internet, strumenti di comunicazione online e strumentazione personale

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.

Il **diritto di accesso a Internet** è 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.

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 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").**

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

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.

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.

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".

Secondo il codice penale italiano i comportamenti penalmente rilevanti in questi casi sono:

- percosse (art. 581),
- lesione personale (art. 582),
- ingiuria (art. 594),
- diffamazione (art. 595),
- violenza privata (art. 610),
- minaccia (art. 612),
- danneggiamento (art. 635).

Nei casi più gravi, basta la denuncia ad un organo di polizia o all'autorità giudiziaria per attivare un procedimento penale (per es. lesioni gravi, minaccia grave, molestie); negli altri casi, la denuncia deve contenere la richiesta che si proceda penalmente contro l'autore di reato (querela).

Capitolo 5 - Segnalazione e gestione dei casi

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. 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.

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.

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.

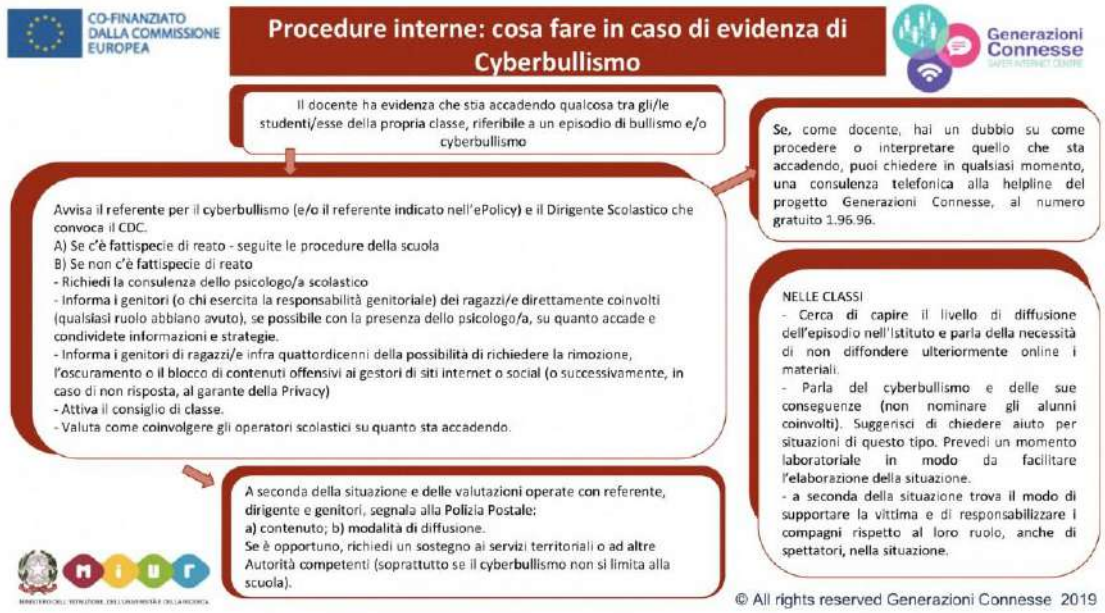
Come descritto nelle procedure di questa sezione, si potrebbero palesare due casi:

- 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.

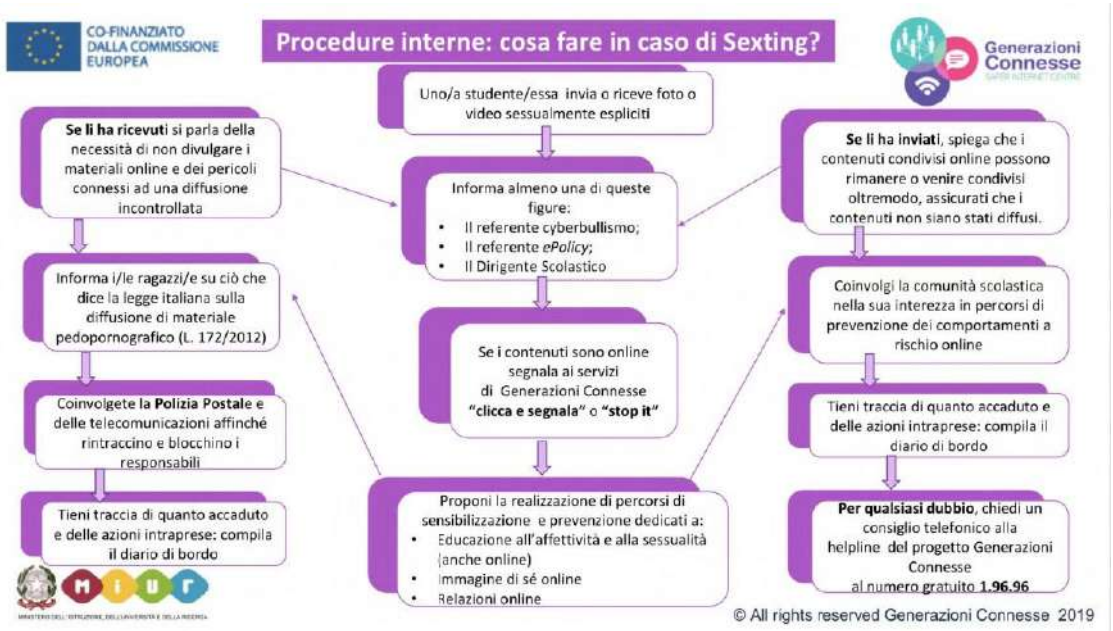
Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione:

- 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.

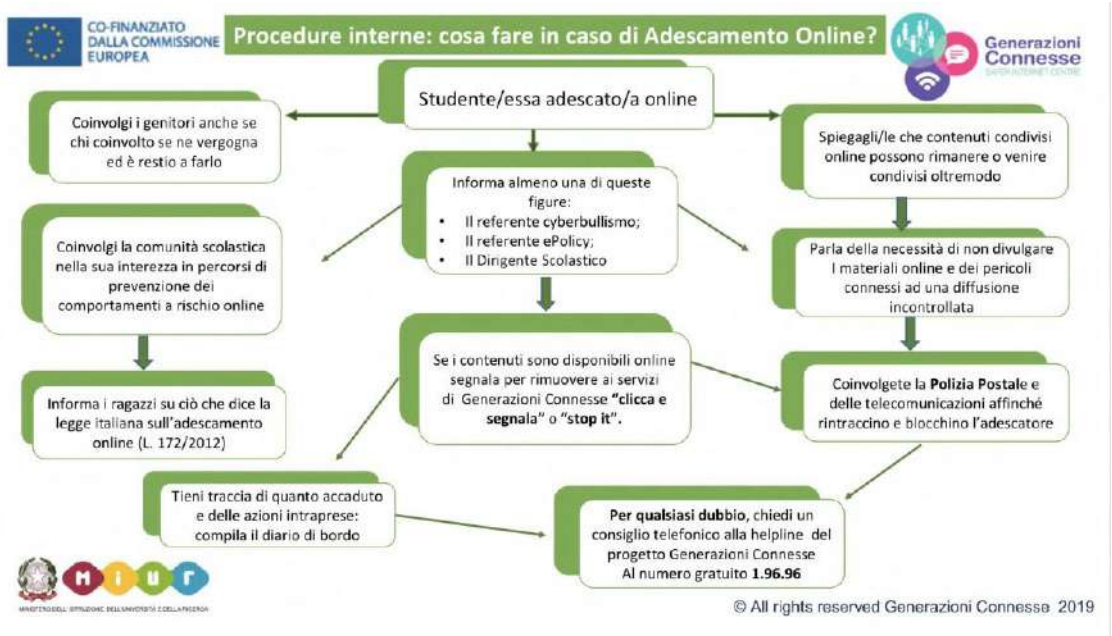
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



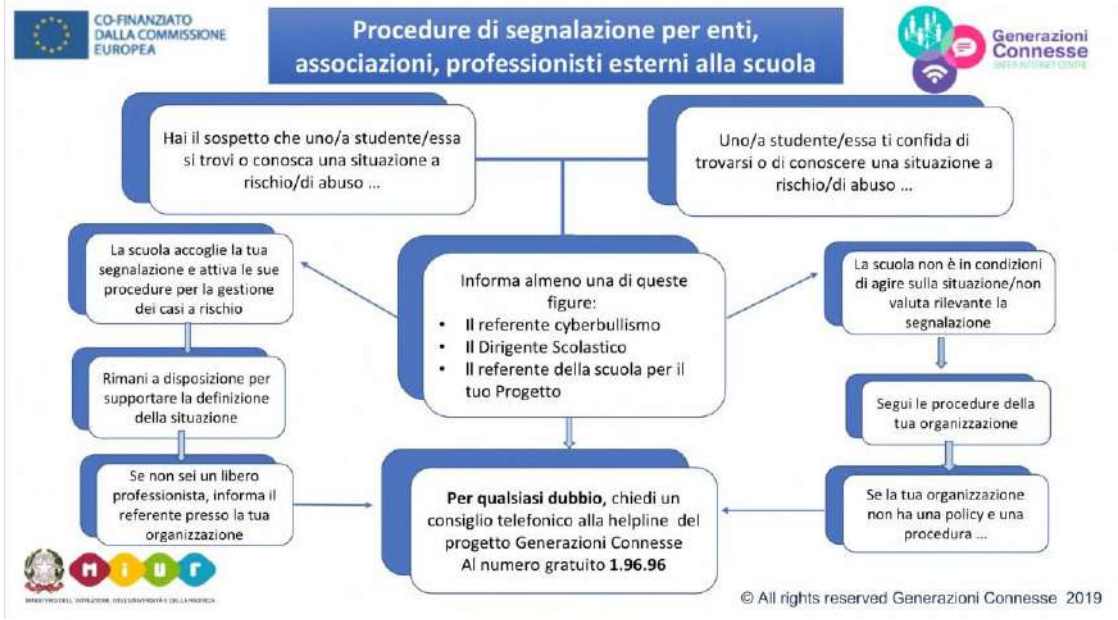
Procedure interne: cosa fare in caso disexting?



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