



Documento di e-Safety Policy

l'orientamento della scuola in materia di sicurezza informatica

LICEO CLASSICO STATALE A. MANZONI
LECCO

Indice del Documento di e-Policy

1. Presentazione e introduzione

- 1.1. Scopo dell'e-Policy
- 1.2. Ruoli e responsabilità
- 1.3. Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto
- 1.4. Condivisione e comunicazione dell'e-Policy all'intera comunità scolastica
- 1.5. Gestione delle infrazioni dell'e-Policy
- 1.6. Integrazione dell'e-Policy con regolamenti esistenti
- 1.7. Monitoraggio dell'implementazione dell'e-Policy e suo aggiornamento

2. Formazione e curriculum

- 2.1. Curriculum sulle competenze digitali per gli studenti
- 2.2. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica e sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali
- 2.3. Sensibilizzazione delle famiglie e Patto di Corresponsabilità

3. Gestione dell'infrastruttura e della strumentazione ICT (Information and Communication Technology) della e nella scuola

- 3.1. Protezione dei dati personali
- 3.2. Accesso ad Internet
- 3.3. Strumenti di comunicazione online
- 3.4. Strumentazione personale

4. Rischi online: conoscere, prevenire e rilevare

- 4.1. Sensibilizzazione e prevenzione
- 4.2. Cyberbullismo: che cos'è e come prevenirlo
- 4.3. Altri rischi online

5. Segnalazione e gestione dei casi

- 5.1. Cosa segnalare
- 5.2. Come segnalare: quali strumenti e a chi
- 5.3. Gli attori sul territorio
- 5.4. Allegati con le procedure

Capitolo 1 - Presentazione del documento di e-Policy

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 riguardo i comportamenti online a rischio;
- le misure per la rilevazione, segnalazione e gestione delle situazioni rischiose legate ad un uso non corretto delle tecnologie digitali.

1.1 Scopo dell'e-Policy

Attraverso l'e-Policy il Liceo Manzoni 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.

Scopo del presente documento di e-Policy è di informare l'utenza per un uso corretto e responsabile delle apparecchiature informatiche collegate alla rete in dotazione alla Scuola, nel rispetto della normativa vigente. In particolare l'intento della scuola è quello di promuovere l'uso consapevole e critico da parte degli alunni delle tecnologie digitali e di Internet, di far acquisire loro procedure e competenze "tecniche", ma anche corrette norme comportamentali, di prevenire ovvero rilevare e fronteggiare le problematiche che derivano da un utilizzo non responsabile, pericoloso o dannoso, delle TIC.

Gli utenti, soprattutto minori, devono essere pienamente consapevoli dei rischi a cui si espongono quando navigano in Rete. Di fatto esiste la possibilità che durante il lavoro online si possa entrare accidentalmente in contatto con materiale inadeguato e/o illegale; pertanto la Scuola promuove l'adozione di strategie che limitino l'accesso a siti e/o applicazioni illeciti. Gli insegnanti hanno la responsabilità di guidare gli studenti nelle attività online a scuola e di indicare regole di condotta chiare per un uso critico e consapevole di Internet anche a casa, per prevenire il verificarsi di situazioni potenzialmente pericolose.

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.

DIRIGENTE SCOLASTICO

Il ruolo del Dirigente Scolastico nel promuovere l'uso consentito delle tecnologie e di Internet include i seguenti compiti:

- garantire la sicurezza (tra cui la sicurezza online) dei membri della comunità scolastica;
- garantire che tutti gli insegnanti ricevano una formazione adeguata per svolgere efficacemente l'insegnamento volto a promuovere una cultura dell'inclusione, del rispetto dell'altro/a e delle differenze, un utilizzo positivo e responsabile delle Tecnologie dell'Informazione e della Comunicazione (TIC);
- gestire i casi di uso improprio delle tecnologie digitali degli studenti e delle studentesse.

ANIMATORE DIGITALE E TEAM DIGITALE

L'Animatore digitale e il Team Digitale si occupano prevalentemente di:

- promuovere la formazione interna all'istituzione negli ambiti di sviluppo della "scuola digitale" e fornire consulenza e informazioni al personale in relazione ai rischi online e alle misure di prevenzione e gestione degli stessi;
- collaborare nel monitorare e rilevare le problematiche legate all'uso sicuro delle tecnologie digitali e di Internet a scuola, nonché proporre la revisione delle politiche dell'istituzione con l'individuazione di soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola.

REFERENTE DI ISTITUTO PER LA PREVENZIONE ED IL CONTRASTO DEL BULLISMO E DEL CYBERBULLISMO

Il referente di Istituto per la prevenzione ed il contrasto del Bullismo e del Cyberbullismo, individuato ai sensi dell'art. 4, comma 3, Legge 29 maggio 2017, n. 71, ha il compito di:

- coordinare le iniziative di prevenzione e di contrasto del cyberbullismo, anche avvalendosi della collaborazione delle Forze di Polizia, nonché delle associazioni e dei centri di

aggregazione giovanile presenti sul territorio.

- essere punto di riferimento non solo in ambito scolastico, ma anche in quello extrascolastico, per l'individuazione di percorsi formativi destinati a studenti e studentesse, genitori e all'intera comunità scolastica.

PERSONALE AMMINISTRATIVO, TECNICO E AUSILIARIO

Il Personale Amministrativo, Tecnico ed Ausiliario (ATA), in collaborazione con il Dirigente Scolastico e con il personale docente tutto, segnala comportamenti non adeguati e/o episodi di bullismo/cyberbullismo alle figure interne preposte.

DOCENTI

Il ruolo del personale docente e di ogni figura educativa che lo affianca include i seguenti compiti:

- informarsi/aggiornarsi sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di Internet e sulla politica di sicurezza adottata dalla scuola, rispettandone il Regolamento e garantire che le modalità di utilizzo corretto e sicuro delle TIC e di Internet siano integrate nel curriculum di studio e nelle attività didattiche ed educative delle classi;
- garantire che gli alunni capiscano e seguano le regole per prevenire e contrastare l'utilizzo scorretto e pericoloso delle TIC e di Internet e assicurare che abbiano una buona comprensione delle opportunità di ricerca offerte dalle tecnologie digitali e dalla rete, ma anche della necessità di evitare il plagio e di rispettare la normativa sul diritto d'autore;
- garantire che le comunicazioni digitali dei docenti con alunni e genitori siano svolte nel rispetto del codice di comportamento professionale ed effettuate con sistemi scolastici ufficiali;
- assicurare la riservatezza dei dati personali trattati ai sensi della normativa vigente e controllare l'uso delle tecnologie digitali, dispositivi mobili, macchine fotografiche, ecc. da parte degli alunni durante le lezioni e ogni altra attività scolastica (ove consentito);
- nelle lezioni in cui è programmato l'utilizzo di Internet, guidare gli alunni a siti controllati e verificati come adatti per il loro uso e controllare che nelle ricerche su Internet siano trovati e trattati solo materiali idonei;
- comunicare ai genitori difficoltà, bisogni o disagi espressi dagli alunni (ovvero valutazioni sulla condotta non adeguata degli stessi) rilevati a scuola e connessi all'utilizzo delle TIC, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo;
- segnalare qualsiasi problema o proposta di carattere tecnico-organizzativo, ovvero esigenza di carattere informativo all'Animatore digitale e al Team Digitale, ai fini della ricerca di soluzioni metodologiche e tecnologiche innovative da diffondere nella scuola e di un aggiornamento della politica adottata in materia di prevenzione e gestione dei rischi nell'uso delle TIC;
- segnalare al Dirigente Scolastico, al referente per il cyberbullismo e ai genitori qualsiasi abuso rilevato a scuola nei confronti degli alunni e del personale scolastico, in relazione

all'utilizzo delle tecnologie digitali o di Internet, per l'adozione delle procedure previste dalle norme.

ALUNNI

Agli alunni si richiede di:

- essere responsabili nell'utilizzo dei sistemi delle tecnologie digitali, in conformità con quanto richiesto dai docenti;
- avere una buona comprensione delle potenzialità offerte dalle TIC per la ricerca di contenuti e materiali, ma anche della necessità di evitare il plagio e rispettare i diritti d'autore;
- comprendere l'importanza di adottare buone pratiche di sicurezza online quando si utilizzano le tecnologie digitali;
- adottare condotte rispettose degli altri anche quando si comunica in Rete;
- esprimere ai docenti e ai genitori domande o difficoltà o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o di Internet.

GENITORI

Ai genitori si richiede di:

- sostenere la linea di condotta adottata dalla scuola in riferimento all'utilizzo delle Tecnologie dell'Informazione e delle Comunicazioni nella didattica;
- concordare con i docenti linee di intervento coerenti e di carattere educativo in relazione ai problemi rilevati per un uso non responsabile o pericoloso delle tecnologie digitali o di Internet;
- favorire un dialogo educativo ai fini dell'utilizzo corretto e responsabile dei dispositivi con accesso a Internet.

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. Inoltre devono 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. E' altrettanto inaccettabile tollerare o farsi coinvolgere in situazioni che sono illegali, o abusive, o che mettano a rischio la sicurezza dei minori.

Tutti gli attori esterni sono tenuti a conoscere e rispettare le regole dell'Istituto che esplicitano le modalità di utilizzo dei propri dispositivi personali (smartphone, tablet, PC, ecc.) 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, anche per quanto riguarda fotografie, immagini, video, o scambio di contatti personali (numero, mail, chat, profili di social network).

1.4 Condivisione e comunicazione dell'e-Policy 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/le 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.

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

Condividere e comunicare la politica di e-safety agli alunni

- tutti gli alunni saranno informati che, a scuola, l'utilizzo di Internet e di ogni dispositivo digitale sarà autorizzato e controllato dagli insegnanti.
- l'istruzione degli alunni riguardo all'uso responsabile e sicuro di Internet precederà l'accesso alla Rete.

Condividere e comunicare la politica di e-safety al personale scolastico

- la linea di condotta della scuola in materia di sicurezza nell'utilizzo delle tecnologie digitali e di Internet sarà discussa negli organi collegiali e comunicata formalmente a tutto il personale con il presente documento e altro materiale informativo anche sul sito web;
- per proteggere tutto il personale e gli alunni, la scuola metterà in atto una linea di condotta di utilizzo limitato alle esigenze didattiche;
- il personale docente sarà reso consapevole del fatto che il traffico in Internet può essere monitorato e si potrà risalire al singolo utente registrato; un'adeguata informazione/formazione del personale docente nell'uso sicuro e responsabile di Internet, sia professionalmente che personalmente, sarà fornita a tutto il personale, anche attraverso il sito web della scuola;
- l'utilizzo delle TIC sarà supervisionato dall'Animatore digitale e dal Team Digitale, che segnaleranno al DSGA eventuali problemi che dovessero richiedere acquisti o interventi di tecnici;
- tutto il personale è consapevole che una condotta non in linea con il codice di comportamento dei pubblici dipendenti e i propri doveri professionali è sanzionabile.

Condividere e comunicare la politica di e-safety ai genitori

- i genitori verranno informati sulla sicurezza nell'uso delle tecnologie digitali e di Internet tramite i mezzi di comunicazione ufficiali dell'Istituto;
- sarà incoraggiato un approccio di collaborazione nel perseguimento della sicurezza nell'uso delle TIC e di Internet in occasione degli incontri scuola-famiglia, assembleari, collegiali e individuali;
- in caso di necessità i genitori potranno contare sul supporto tecnico fornito dalla scuola.

1.5 Gestione delle infrazioni della e-Policy

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

Disciplina degli alunni

Sono previsti provvedimenti disciplinari proporzionati all'età e alla gravità del comportamento, secondo quanto indicato nel Regolamento di Disciplina d'Istituto.

Contestualmente sono previsti interventi di carattere educativo di rinforzo dei comportamenti corretti e riparativi dei disagi causati, di ridefinizione 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, se non favorire l'uso scorretto e irresponsabile delle TIC da parte degli alunni.

Tutto il personale è tenuto a collaborare con il Dirigente Scolastico e a fornire ogni informazione utile per le valutazioni del caso e per l'avvio di procedimenti che possano 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 della responsabilità degli adulti nei confronti dei propri figli, anche ai genitori viene richiesta una condotta che favorisca l'uso corretto e responsabile delle TIC da parte degli alunni a scuola e a casa.

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 gli altri.

1.6 Integrazione dell'e-Policy 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.

Disposizioni sull'uso dei software

- i software installati sono ad esclusivo uso didattico;
- è fatto divieto di usare software non conforme alle leggi sul copyright;
- è responsabilità degli insegnanti che chiedono ai tecnici della scuola di effettuare copie di cd/dvd per uso didattico, assicurarsi che la copia non infranga le leggi sul copyright in vigore.

Accesso a Internet

- l'accesso a Internet è consentito al personale docente e non docente solo ad esclusivo uso didattico e/o di formazione e sotto la responsabilità di un insegnante;
- Internet non può essere usato per scopi vietati dalla legislazione vigente e l'utente è responsabile dell'uso fatto, civilmente e penalmente;
- è vietato inserire sui PC connessi in Rete programmi contenenti virus, scaricare da Internet software non autorizzati, scaricare e installare software senza licenza. Chiunque verifichi un uso delle TIC non conforme alle disposizioni di legge o al Regolamento interno deve darne comunicazione per iscritto al Dirigente Scolastico.

1.7 Monitoraggio dell'implementazione della e-Policy 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 tutto il 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.

La scuola affida al referente per l'e-Policy il ruolo di confrontarsi con un gruppo di lavoro specifico e monitorare l'implementazione della e-Policy e il suo aggiornamento.

Capitolo 2 - Formazione e curriculum

2.1. Curriculum 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 alle 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 ad un uso consapevole e responsabile delle tecnologie digitali. Ciò avverrà attraverso la progettazione e implementazione di un curriculum digitale. La formazione del curriculum digitale non può non tener conto di quanto disposto dall’art. 5 della Legge 20 agosto 2019 n. 92 (Introduzione dell’insegnamento scolastico dell’educazione civica) interamente dedicato alla “cittadinanza digitale”, intesa come capacità di un individuo di avvalersi consapevolmente e responsabilmente dei mezzi di comunicazione virtuali.

2.2 Formazione dei docenti sull’utilizzo e l’integrazione delle TIC nella didattica e sull’utilizzo consapevole e sicuro di Internet e delle tecnologie digitali

È fondamentale che i docenti 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.

Nel corso degli anni, presso l’Istituto è stato favorito l’inserimento delle tecnologie informatiche nella didattica (registro elettronico, LIM, ambienti di condivisione, laboratori informatici mobili) nella prospettiva dell’inclusione, non solo in relazione ai Bisogni Educativi Speciali, ma più in generale per facilitare un percorso di apprendimento in grado di promuovere il successo formativo.

Tutti i docenti dell’Istituto hanno svolto e continuano a svolgere attività di formazione per un corretto utilizzo dei dispositivi digitali e delle piattaforme per la didattica.

La scuola si impegna, inoltre, a promuovere percorsi formativi per gli insegnanti sul tema dell’uso consapevole delle tecnologie digitali e della prevenzione dei rischi online, monitorando le azioni svolte per mezzo di specifici momenti di valutazione.

La formazione avverrà tramite incontri di aggiornamento che verranno organizzati dall’Istituto scolastico con la collaborazione del personale specializzato interno (Animatore Digitale, Team

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, ecc...), delle amministrazioni comunali, dei servizi socio-educativi e delle associazioni presenti.

Sul sito istituzionale della scuola è presente il link a *Generazioni Connesse*, utile per approfondimenti, spunti, aggiornamenti e strumenti didattici da usare con gli studenti e le studentesse.

2.3 - Sensibilizzazione delle famiglie e integrazioni al Patto di Corresponsabilità

L'Istituto garantisce alle famiglie la massima informazione riguardante tutte le attività e iniziative intraprese sul tema delle tecnologie digitali, previste dall'e-Policy e dal suo piano di azioni, attraverso l'aggiornamento del Regolamento scolastico e del Patto di Corresponsabilità, e attraverso una sezione dedicata sul sito web dell'Istituto.

AZIONI

- organizzazione di incontri con esperti sulle competenze digitali, sull'educazione alla cittadinanza digitale;
- raccolta dei suggerimenti dei genitori per individuare i temi di maggiore interesse nell'ambito dell'educazione alla cittadinanza digitale;
- organizzazione e promozione di incontri formativi per il corpo docente sull'utilizzo consapevole e sicuro di Internet e sulle 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 riguardanti gli studenti e le 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 relazione al nuovo Regolamento Generale sulla Protezione dei Dati, (UE) 679/2016 “GDPR” con effetti diretti a partire dal 25 maggio 2018, recepito in Italia col decreto legislativo n.101 del 10-08-2018, vigente dal 19 settembre 2018, che inserisce la figura obbligatoria nella P.A. del Responsabile della Protezione dei Dati (RPD), per agevolare l'applicazione del GDPR. Il nostro Istituto ha provveduto alla nomina di Luca Corbellini, Data Protection Officer, Specialista in Informatica Giuridica e Sicurezza del Lavoro Studio AG.I.COM. S.r.l. - Via XXV Aprile, 12 - 20070 SAN ZENONE AL LAMBRO (MI), Tel. 02-90601324 - FAX 02-700527180 - <http://www.agicomstudio>.

Il nostro Istituto si è prontamente adeguato alla suindicata normativa adempiendo a quanto in essa prescritto.

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 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.

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. Il nostro Istituto è dotato, attualmente, di strumenti di comunicazione esterna e interna.

Fra gli strumenti di comunicazione sia interna che esterna troviamo il sito web della scuola, il registro elettronico e la posta elettronica, applicativi e piattaforme che hanno favorito un lavoro collaborativo e condiviso rendendo possibile un agevole passaggio alla didattica a distanza nel periodo di lockdown.

In riferimento all'uso degli strumenti di comunicazione online per la circolazione di informazioni e comunicazioni interne è importante ricordare quello che si può definire "diritto alla disconnessione". L'art. 22 (Livelli, soggetti, materie di relazioni sindacali per la Sezione Scuola) del CCNL 2016/2018, infatti, fa riferimento ai criteri generali per l'utilizzo di strumentazioni tecnologiche di lavoro in orario diverso da quello di servizio, al fine di una maggiore conciliazione fra vita lavorativa e vita familiare.

3.4 Strumentazione personale

Il nostro Istituto si è dotato di una regolamentazione condivisa e specifica su tali aspetti per la quale si rinvia al Regolamento di Istituto e al Regolamento per la DDI.

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.

Appare chiaro come le migliori strategie di intervento a garanzia della sicurezza, siano di carattere prevalentemente preventivo.

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;
- 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;
- predisposizione di azioni preventive ed educative e non solo sanzionatorie.

È molto importante sottolineare come il cyberbullismo non sia una problematica che riguarda unicamente vittima e cyberbullo. È un fenomeno sociale e di gruppo.

Il Referente per le iniziative di prevenzione e contrasto ha il compito di coordinare le iniziative di prevenzione e contrasto del [cyberbullismo](#). A tal fine, si avvale della collaborazione delle Forze di polizia, delle associazioni e dei centri di aggregazione giovanile del territorio e di altre agenzie educative.

Il referente svolge anche un importante compito di supporto al Dirigente Scolastico per la revisione/stesura di Regolamenti (Regolamento d'Istituto), Atti e Documenti (PTOF, PdM, Rav).

4.3. - Altri rischi online

Anche per prevenire gli altri fenomeni di rischio (hate speech, sexting, dipendenze, adescamento, pedopornografia, ...) la scuola si impegna a compiere percorsi di prevenzione e sensibilizzazione all'uso corretto e consapevole di Internet e dei dispositivi elettronici, attraverso il curricolo di Educazione Civica.

Fondamentale è implementare un percorso di educazione digitale che comprenda lo sviluppo anche di capacità quali la protezione della propria privacy e la gestione dell'immagine e dell'identità online, la capacità di gestire adeguatamente le proprie relazioni online, a partire dalla consapevolezza della peculiarità del mezzo/schermo che permette a chiunque di potersi presentare molto diversamente da come realmente è.

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 o altro, ha a disposizione procedure definite e può fare riferimento a tutta la comunità scolastica.

Questa sezione dell'e-Policy 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'e-Policy).

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 all bullismo e al 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 la scuola prevede 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, utilizzando di locandine da affiggere a scuola, pubblicate le news nel sito della scuola, in occasione dei 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? ecc.). È necessario poi valutare l'eventuale stato di disagio vissuto dagli/le 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 minorenni e inoltre è importante non sostituirsi all'adolescente, evitando, quindi, di rispondere all'adescatore al suo posto. È fondamentale valutare il benessere psicofisico dei minori e il rischio che corrono. 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 prodotti autonomamente da persone minorenni, sfuggano al loro controllo e vengano diffusi 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 dei 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.

I seguenti servizi possono essere di supporto alle problematiche citate:

- 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.

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 svolgimento 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 si faccia 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 *ad hoc* messi a loro disposizione:

- un indirizzo e-mail specifico per le segnalazioni;
- sportello di counseling psicologico;
- docente referente per le segnalazioni.

Studenti e studentesse, inoltre, possono rivolgersi alla *Helpline* del progetto Generazioni Connesse, al numero gratuito [1.96.96](tel:19696).

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.

Per il territorio di Lecco:

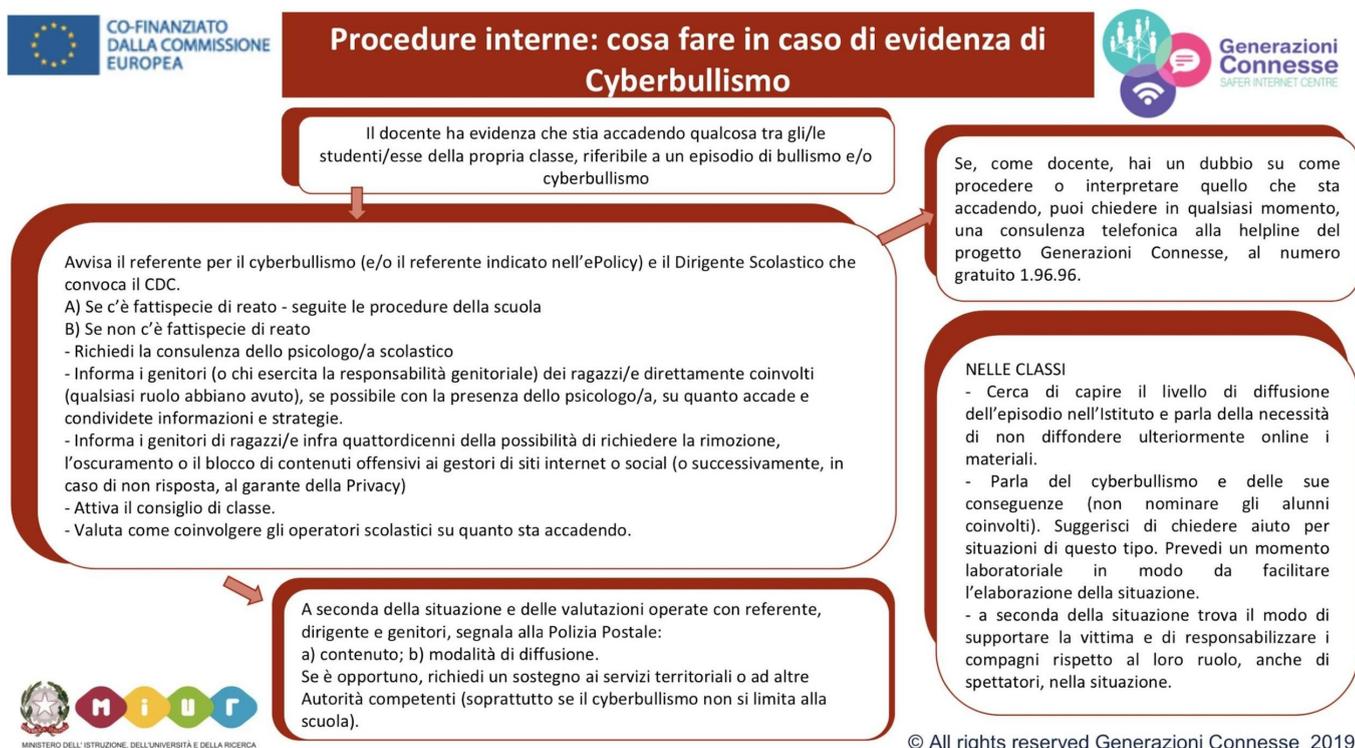
- Il **servizio di ascolto psicologico** dedicato ai ragazzi **dai 15 ai 24 anni** tenuto da un'équipe esperta di **psicologi di ASST Lecco - Ospedale "A. Manzoni"**, con accesso è **libero e gratuito**. **Sede di Lecco:** via dell'Eremo 28, cell. 333.6163136, e-mail: quindiciventiquattro.lecco@asst-lecco.it.
- **Sportello telefonico di supporto psicologico** del Comune di Lecco per crisi acute e situazioni di urgenza, libero e gratuito. Tel. 335 6735471, da mercoledì a domenica, dalle 9 alle 21.

5.4 Allegati con le procedure

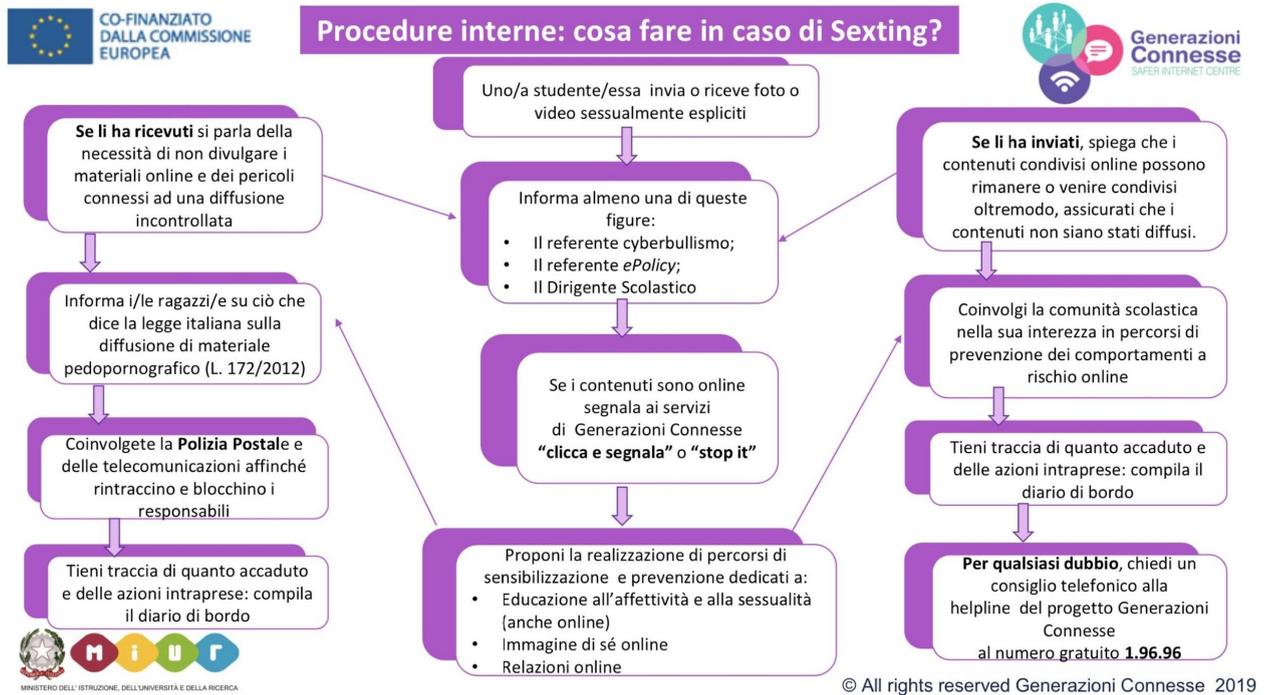
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



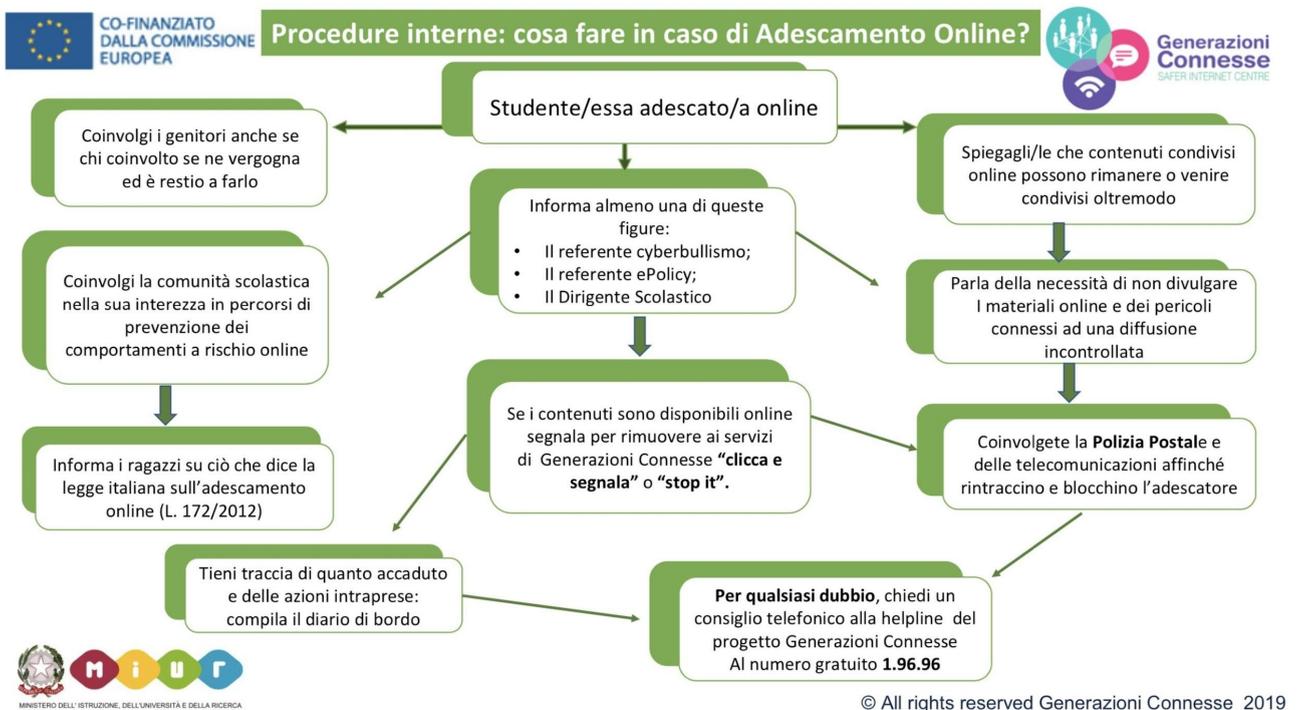
Procedure interne: cosa fare in caso di evidenza di Cyberbullismo?



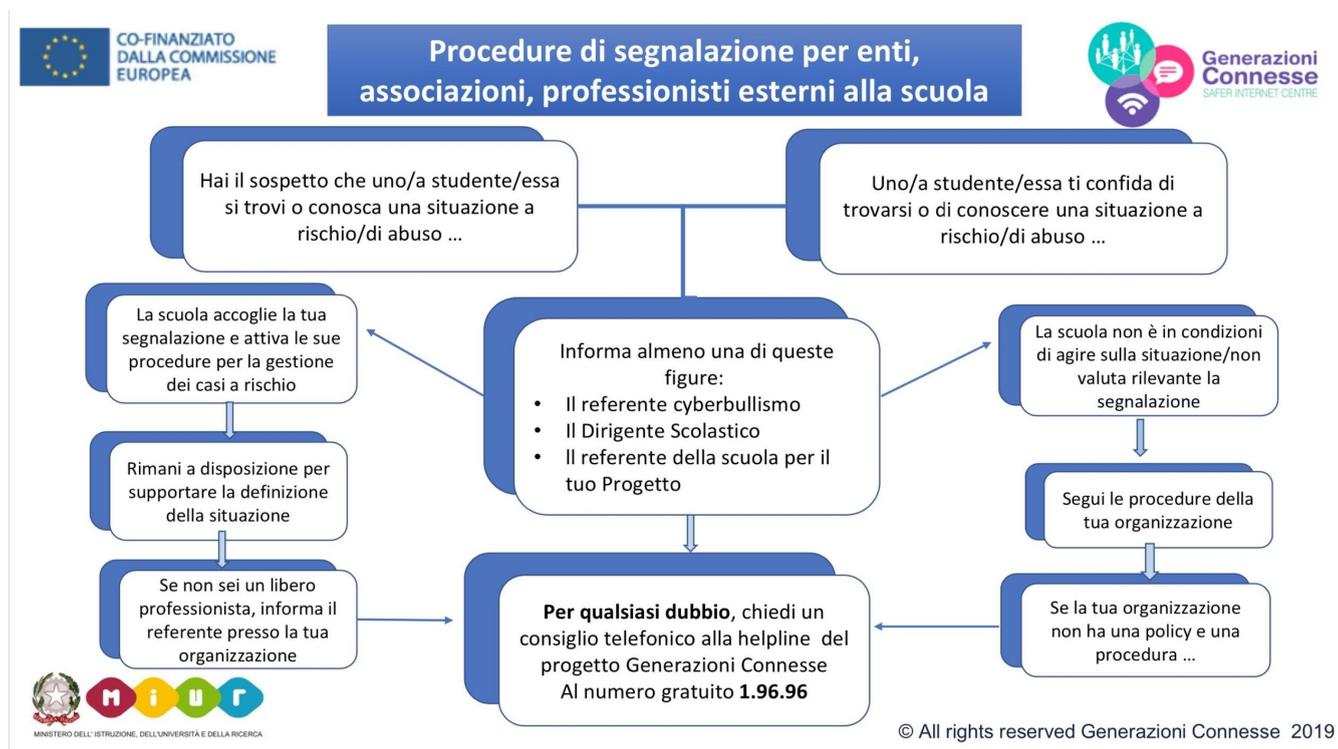
Procedure interne: cosa fare in caso di sexting?



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](#)