# Documento di ePolicy

AVIC87000C

I.C. "R. GUARINI"

PIAZZA MANZONI - 83036 - MIRABELLA ECLANO - AVELLINO (AV)

MARIA ULLUCCI

# 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.

L'Istituto Comprensivo Statale "Raimondo Guarini" ha elaborato questo documento in conformità con le Linee di Orientamento per la prevenzione e il contrasto dei fenomeni di Bullismo e Cyberbullismo del 13/01/2021, con l'obiettivo di educare e sensibilizzare gli alunni, gli insegnanti e i genitori all'uso sicuro e consapevole di Internet. Infatti lo sviluppo delle Nuove Tecnologie, il loro utilizzo nell'ambito didattico e la maggiore diffusione nella vita di tutti i giorni di questi strumenti richiede maggiore responsabilità e consapevolezza. È compito dell'intera comunità scolastica, genitori inclusi, garantire che gli studenti siano in grado di utilizzare le tecnologie digitali e che lo facciano in modo appropriato e sicuro. Di qui la necessità di dotare la scuola di una propria Policy di E-safety, per gestire le eventuali infrazioni come integrazione del Regolamento d'Istituto.

La Policy di E-safety permette di regolare il comportamento degli alunni dentro e fuori dalle aule scolastiche, sensibilizzandoli con idonei interventi formativi all'adozione di buone pratiche e prevedendo sanzioni disciplinari per comportamenti inappropriati e/o addirittura illeciti avvenuti all'interno dell'istituzione scolastica.

Il documento prevede le seguenti linee di intervento:

- l'elaborazione di linee guida per una E-safety Policy d'istituto, cioè un proprio codice di condotta nella prevenzione e gestione dei casi di bullismo e di cyberbullismo;
- l'individuazione di regole di sicurezza informatica per tutti i membri della comunità scolastica, attenendosi alle linee di orientamento proposte dal MIUR;
- la procedura per la gestione di situazioni problematiche e le attività di prevenzione;
- la promozione, negli alunni, della competenza digitale e della cultura del rispetto di regole comuni nell'uso della tecnologia e lo sviluppo di norme comportamentali.

---

# *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:

- garantisce la tutela degli aspetti legali riguardanti la privacy e la tutela dell'immagine di tutti i membri della comunità scolastica;
- garantisce ai propri docenti una formazione di base sulle tecnologie dell'Informazione e della Comunicazione (ICT) che consenta loro di possedere le competenze necessarie all'utilizzo di tali risorse;
- garantisce l'esistenza di un sistema che consenta il monitoraggio e il controllo interno della sicurezza on- line;
- garantisce che la scuola utilizzi un Internet Service filtrato, approvato, conforme ai requisiti di legge;
- informa tempestivamente, qualora venga a conoscenza di atti di cyberbullismo che non si configurino come reato, i genitori dei minori coinvolti; (o chi ne esercita la responsabilità genitoriale o i tutori);
- gestisce e interviene nei casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali;
- ha un ruolo di primo piano nello stabilire e rivedere la E-policy.

L'Animatore digitale e il suo team ha i seguenti compiti:

- stimola la formazione interna all'istituzione negli ambiti di sviluppo della " scuola digitale" e fornisce informazioni al personale in relazione ai rischi online e alle misure di prevenzione e gestione degli stessi;
- assicura che gli utenti possano accedere alla rete della scuola solo tramite password applicate e regolarmente cambiate e cura lo sviluppo del sito web della scuola per scopi istituzionali e consentiti (istruzione e formazione );

- coinvolge la comunità scolastica (alunni, genitori e altri) nella partecipazione ad attività e progetti attinenti la "scuola digitale";
- pubblica la e-policy sul sito della scuola;
- diffonde la conoscenza dell'e-policy;
- garantisce che tutti i dati relativi agli alunni pubblicati sul sito siano sufficientemente tutelati

Referente Cyberbullismo d'Istituto:

- coordina iniziative di prevenzione e contrasto del cyberbullismo messe in atto dalla scuola;
- predispone un documento di rilevazione di incidenti di sicurezza in rete;
- facilita la formazione e la consulenza di tutto il personale.

Insegnanti:

- provvedono personalmente alla propria formazione/aggiornamento sull'utilizzo del digitale con particolare riferimento alla dimensione etica (tutela della privacy, rispetto dei diritti intellettuali dei materiali reperiti in internet e dell'immagine degli altri: lotta al cyberbullismo);
- supportano gli alunni nell'utilizzo consapevole delle tecnologie informatiche utilizzate a scopi didattici;
- segnalano al Dirigente Scolastico e ai suoi collaboratori eventuali episodi di violazione delle norme di comportamento stabilite dalla scuola, avviando le procedure previste in caso di violazione;
- supportano ed indirizzano alunni coinvolti in problematiche legate alla rete.

Personale amministrativo, tecnico ausiliario (ATA):

- segnala comportamenti non adeguati e/o episodi di bullismo/cyberbullismo;

- garantisce il funzionamento dei diversi canali di comunicazione della scuola (sportello, circolari, sito web,…) all'interno della scuola e fra la scuola e le famiglie degli alunni per la notifica di documenti e informazioni del DS e dell'Animatore digitale nell'ambito dell'uso delle tecnologie;

- ha la responsabilità per i problemi di sicurezza online (uffici amministrativi…);

- controlla la condivisione di dati personali e l'accesso a materiali illegali/inadeguati.

Genitori:

contribuiscono, in sinergia con il personale scolastico, alla sensibilizzazione dei propri figli sul tema della sicurezza in rete;

- incoraggiano l'impiego delle ICT da parte degli alunni nello svolgimento dei compiti a casa, controllando che tale impiego avvenga in sicurezza;

- agiscono in modo concorde con la scuola per la prevenzione dei rischi e l'attuazione delle procedure previste in caso di violazione delle regole stabilite;

- rispondono per gli episodi commessi dai figli minori a titolo di culpa in educando (articolo 2048 del Codice Civile). Sono esonerati da responsabilità solo se dimostrano di non aver potuto impedire il fatto.

Gli alunni in relazione al proprio grado di maturità e consapevolezza raggiunta:

- sono responsabili nell'uso delle tecnologie digitali in coerenza con quanto richiesto dai docenti;

- comprendono le potenzialità offerte dalle TIC ma anche la necessità di evitare il plagio e rispettare i diritti d'autore;

- conoscono i rischi e i benefici di utilizzo delle tecnologie per usarle in modo sicuro sia a scuola che a casa;

- comprendono l'importanza di segnalare abusi, l'uso improprio o l'accesso a materiali inappropriati;

- riconoscono quale sia l'uso corretto dei cellulari, fotocamere digitali, dispositivi portatili;

- comprendono la politica della scuola sull'uso di immagini e il cyberbullismo;
- adottano condotte rispettose degli altri anche quando si comunica in rete.

Gli enti educativi esterni e le Associazioni

gli Enti educativi esterni e le associazioni che entrano in relazione con la scuola devono conformarsi alla politica della stessa riguardo all'uso consapevole della Rete e delle TIC; devono, inoltre, promuovere comportamenti sicuri, la sicurezza online e assicurare la protezione degli studenti e delle studentesse durante le attività che si svolgono insieme.

---

# *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).

Le organizzazioni/associazioni extrascolastiche e gli esperti esterni chiamati, a vario titolo, alla realizzazione di progetti ed attività educative, sul breve o/e lungo periodo, dovranno prendere atto di quanto stilato nell' E-policy dell'Istituto o eventualmente sottoscrivere un'informativa sintetica del documento in questione, presente nel contratto.

# 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 E-Safety Policy d'istituto si applica a tutti i membri della scuola:

Agli alunni: prima di accedere alla rete tutti gli alunni saranno informati che la rete, l'uso di internet e di ogni altro dispositivo digitale saranno controllati dai docenti e utilizzati solo con la loro autorizzazione;

Al personale:

- la linea di condotta della scuola in materia di sicurezza nell'utilizzo delle tecnologie sarà discussa negli organi collegiali e comunicata a tutto il personale con il presente documento;

- per proteggere tutto il personale la scuola metterà in atto una linea di condotta di utilizzo accettabile, controllato e limitato alle esigenze didattiche;

- sarà fornita una informazione/formazione sull'uso sicuro e responsabile di internet;

- l'utilizzo delle TIC sarà supervisionato dall'Animatore digitale, che segnalerà al DSGA eventuali problemi che dovessero richiedere acquisti o interventi di tecnici;

- tutto il personale è tenuto ad uniformarsi alla linea di condotta della scuola, in violazione del codice di comportamento la condotta è sanzionabile.

Ai genitori:

- 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;

- l'Animatore digitale fornirà indicazioni sull'uso sicuro delle TIC;

- il DS avrà il compito di informare i genitori circa episodi di comportamento inappropriato di sicurezza online (es. Cyberbullismo).

La Policy sarà comunicata alla comunità nei seguenti modi:

- pubblicato sul sito della scuola;

- discusso, accettato e sottoscritto dai genitori tramite il Patto di corresponsabilità;

- accettato da tutto il personale scolastico.

---

# *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.

La scuola metterà in atto tutte le azioni necessarie per garantire agli studenti l'accesso sicuro adottando tutti i sistemi di sicurezza conosciuti per diminuire le possibilità di rischio durante la navigazione. Pur consapevoli che non è possibile garantire una navigazione totalmente priva di rischi sia la scuola sia gli insegnanti non possono assumersi le responsabilità conseguenti all'accesso accidentale a siti illeciti.

Comunque le potenziali infrazioni in cui gli alunni possono incorrere a scuola nell'utilizzo delle TIC sono:

- uso della rete per aggredire, molestare, denigrare, giudicare qualcuno;
- acquisizione illecita e invio senza permesso di foto o di altri dati personali come indirizzo di casa o telefono;
- comunicazione incauta e senza permesso con sconosciuti;
- collegamenti a siti web non indicati dai docenti;
- utilizzare la rete per interessi privati e personali che esulano dalla didattica;
- scaricare file, video-musicali protetti da copyright;
- deridere, offendere, insultare, calunniare e minacciare attraverso l'uso delle TIC;
- pubblicare sui social network o inviare tramite messaggistica immagini, video o testi che siano offensivi della dignità personale;
- attuare cyberstalking o altre forme di persecuzione e molestia attraverso l'uso delle TIC.

Gli interventi correttivi previsti sono rapportati all'età e al livello di sviluppo dell'alunno.

Il nostro istituto essendo comprensivo, si rivolge ad alunni di età compresa tra i 3 e i 13 anni, perciò gli interventi, sono diretti a correggere quei comportamenti dovuti a uno sviluppo cognitivo, affettivo e morale incompleto oppure a fasi critiche transitorie, e sono diretti a sviluppare una maggiore consapevolezza e maturità dell'alunno.

Sono previsti pertanto dei provvedimenti "disciplinari":

- il richiamo verbale
- il richiamo scritto
- la convocazione dei genitori da parte dei docenti
- la convocazione dei genitori da parte del DS
- la sospensione dalle lezioni
- la segnalazione agli assistenti sociali
- la segnalazione alle autorità competenti in caso di reati.

Contestualmente sono previsti anche interventi educativi diretti al recupero delle regole sociali di convivenza civile attraverso la partecipazione attiva e consapevole degli alunni, di prevenzione e di gestione positiva dei conflitti, di moderazione dell'eccessiva competitività, di promozione dei rapporti di amicizia, di promozione e conoscenza delle emozioni, e interventi di educazione al rispetto degli altri e del diverso, alla solidarietà e alla collaborazione, e di educazione all'affettività.

L'infrazione della presente E-Policy da parte del personale (docente, ATA,) può costituire elemento di contestazione d'addebito disciplinare e per gli esterni (esperti, collaboratori, etc.) può essere causa di risoluzione di eventuali contratti e/o convenzioni in essere.

---

# *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 si integra con il Regolamento di istituto in riferimento alle norme comportamentali relative all'uso delle TIC, con il PDM e con il PTOF.

---

# 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.

Il monitoraggio dell'implementazione della policy e del suo eventuale aggiornamento sarà svolto ogni anno e sarà curato dal DS con la collaborazione dell'Animatore digitale, dal docente per la sicurezza e dai docenti delle classi tramite questionari e conversazioni.

Attività previste:

- test sondaggio per monitorare le abitudini di internet degli alunni e per rilevare il livello di conoscenza dei rischi di internet e della consapevolezza degli strumenti esistenti per tutelarsi;
- test sulla sicurezza in internet attraverso il supporto dei kit didattici messi a disposizione nell'area del sito "generazioni connesse";
- organizzazione di incontri dedicati alla prevenzione dei rischi associati all'utilizzo di internet e delle tecnologie digitali, anche con esperti;
- lezioni sulla privacy, sul bullismo e sul cyberbullismo.

## Il nostro piano d'azioni

### Azioni da svolgere entro un'annualità scolastica:

- Organizzare uno o più eventi o attività volti a presentare il progetto ai rappresentanti dei genitori del Consiglio d'Istituto per la stesura finale dell'ePolicy.
- Organizzare 1 evento di presentazione del progetto Generazioni

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

## Azioni da svolgere nei prossimi 3 anni:

- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i docenti dell'Istituto per la stesura finale dell'ePolicy.
- Organizzare incontri per la consultazione degli studenti/studentesse sui temi dell'ePolicy per cui si evidenzia la necessità di regolamentare azioni e comportamenti.
- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i genitori dell'Istituto per la stesura finale dell'ePolicy.
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto agli studenti
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai docenti
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai genitori
- 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.

## *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.

## 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.

## 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.

## Il nostro piano d'azioni

# 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.

I modelli di liberatoria sono reperibili al seguente link: https://www.icmirabellaeclano.edu.it/index.php/documenti/modulistica

La scuola non ha solo il compito di tutelare la privacy degli/lle studenti/esse e delle loro famiglie, ma anche quello di informare e soprattutto rendere consapevoli gli/le studenti/esse di quanto sia importante tutelare il diritto alla riservatezza di se stessi e degli altri. 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 pubblicarli sul sito istituzionale dell'Istituto. In caso di utilizzo di piattaforme digitali condivise o di strumenti per la creazione e la gestione di classi virtuali, che richiedano l'inserimento di dati sensibili viene acquisito preventivamente il consenso informato dei genitori. In caso di attività di ampliamento dell'offerta formativa, organizzate in collaborazione con Enti esterni, viene richiesto preventivamente ai genitori il consenso informato alle riprese audio/ video e al loro eventuale utilizzo per scopi didattici, informativi e divulgativi anche tramite pubblicazione su siti web. L'accesso ai dati riportati nel registro elettronico (ritardi, assenze, note e valutazioni) è riservato ai genitori della Scuole primarie e alla secondaria di primo grado tramite l'invio di una password di accesso strettamente personale. La diffusione sempre maggiore di smartphone tra i giovanissimi, l'uso di tablet a scopo didattico, la condivisione online di contenuti didattici, l'uso del registro elettronico, l'eventualità di gruppi whatsapp tra studenti/esse, genitori, docenti o tra insegnanti e studenti/esse, obbliga la scuola ad avere un'attenzione particolare non solo alla privacy in generale, ma anche alla gestione della privacy legata all'uso dei nuovi dispositivi. La velocità, l'immediatezza con cui si risponde ai messaggi o si condividono foto o video, può far perdere il controllo di dati personali e mettere a rischio la reputazione e la sicurezza dei soggetti coinvolti. Sono dati personali le informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, etc. I soggetti che procedono al trattamento dei dati personali altrui dunque devono adottare particolari misure per garantire il corretto e sicuro utilizzo dei dati. Le istituzioni scolastiche pubbliche possono trattare solamente i dati personali necessari al perseguimento di specifiche finalità istituzionali, oppure quelli espressamente previsti dalla normativa di settore. Per tali trattamenti non sono tenute a chiedere il consenso degli/lle studenti/esse. Alcune categorie di dati personali degli/lle studenti/esse e delle famiglie, come quelli sensibili e giudiziari, devono essere

trattate invece con estrema cautela, nel rispetto di specifiche norme di legge, verificando in primis non solo la pertinenza e completezza dei dati, ma anche la loro indispensabilità rispetto alle "finalità di rilevante interesse pubblico" che si intendono perseguire. Le scuole, sia pubbliche che private, hanno l'obbligo quindi di informare (tramite apposita informativa) gli interessati delle caratteristiche e modalità del trattamento dei loro dati, indicando i responsabili del trattamento. Gli interessati non sono solo gli/le studenti/esse, ma anche le famiglie e gli stessi professori. È importante, inoltre, che le scuole verifichino i loro trattamenti, controllando se i dati siano eccedenti rispetto alle finalità perseguite. La scuola non è tenuta a richiedere alle famiglie l'autorizzazione alle riprese fotografiche e video (ad es. in caso di gite scolastiche o recite) solo se esse sono realizzate a fini personali e non a fini di pubblicazione o divulgazione: il nostro Istituto è particolarmente attento al sito web della scuola, ma anche alle pagine Facebook o a whatsapp perché si tratta di divulgazione e necessita di autorizzazione degli interessati. In generale il Garante per la protezione dei dati personali stabilisce che "le scuole devono rendere noto alle famiglie e ai ragazzi, attraverso un'adeguata informativa, quali dati raccolgono e come li utilizzano". Famiglie e studenti hanno il diritto di conoscere quali informazioni sono trattate dall'Istituto scolastico, farle rettificare se inesatte, incomplete o non aggiornate.

---

# *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.

La scuola deve dunque considerare l'ambiente online alla stregua dell'ambiente fisico e valutarne tutti gli aspetti legati alla sicurezza nel momento in cui permette a studenti/esse e docenti l'accesso alla rete tramite i dispositivi della scuola, tramite la rete scolastica o tramite i dispositivi personali. In riferimento alla security non è sufficiente prestare attenzione all'infrastruttura hardware e alla rete (wireless e non), ma è necessario considerare anche la sicurezza di tutti gli aspetti che riguardano la gestione degli account degli utenti (in modo differenziato tra studenti, insegnanti e personale amministrativo), il filtraggio dei contenuti (possibilmente in modo differenziato in base all'età) e gli aspetti legali in relazione prevalentemente alla privacy. Data la giovane età degli studenti del nostro Istituto, è fondamentale fare tutto il possibile per evitare l'esposizione a contenuti inappropriati. L'accesso a internet è possibile e consentito per la didattica in tutte le aule e nei laboratori multimediali sia per il docente che per gli alunni, che sono strettamente monitorati. La connessione alla rete wi-fi è riservata ai docenti, che possono utilizzare anche dispositivi personali, per fini didattici. Per tutto il personale della scuola la connessione alla rete wi-fi è accessibile tramite una password. Le postazioni presenti in segreteria sono accessibili solo dal personale amministrativo con utenza e password dedicate. Se l'accesso a Internet è un diritto, esso deve anche essere adeguato all'età degli utenti. L'obiettivo principale resta quello di arricchire ed ampliare le attività didattiche, secondo quanto prevede il curricolo scolastico, l'età e la maturità degli/lle studenti/esse e le indicazioni sono quelle di permettere un utilizzo adeguato delle risorse web per creare un ambiente sicuro, simile a quello "reale" e che permetta agli studenti, fin da piccoli, di affrontare il web con la guida degli insegnanti. Il regolamento di Istituto prevede una parte dedicata all'uso di Internet in cui gli studenti si impegnano a: utilizzare la rete nel modo corretto rispettare le consegne dei docenti non scaricare materiali e software senza autorizzazione non utilizzare unità removibili personali senza autorizzazione tenere spento lo smartphone al di fuori delle attività didattiche che ne prevedano l'utilizzo durante le attività che prevedono lo

smartphone, utilizzarlo esclusivamente per svolgere le attività didattiche previste segnalare immediatamente materiali inadeguati ai propri insegnanti. I docenti si impegnano a: utilizzare la rete nel modo corretto non utilizzare device personali se non per uso didattico formare gli studenti all'uso della rete dare consegne chiare e definire gli obiettivi delle attività monitorare l'uso che gli studenti fanno delle tecnologie a scuola. Per superare la diffidenza nei confronti delle tecnologie a scuola e il divario nell'accesso la scuola provvede a piani di interventi di manutenzione e mira a formare gli insegnanti per permettere loro di affrontare e risolvere in autonomia tutte quelle situazioni e casistiche di mal funzionamento dei dispositivi che si possono presentare nella quotidianità. La parola d'ordine per quanto riguarda le tecnologie è sempre: "formazione". Formazione non solo sull'uso delle tecnologie digitali nella didattica, ma anche sul funzionamento e sull'uso stesso della tecnologia in sé grazie al supporto del tecnico della scuola, in collaborazione con l'animatore digitale e a qualche docente che per studio o passione ha conoscenze più tecniche da poter condividere coi colleghi.

---

# *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.

Fra gli strumenti di comunicazione esterna, troviamo in primis il sito web del nostro Istituto. Fra quelli di comunicazione interna, invece, troviamo il registro elettronico con tutte le sue funzionalità, la classica e-mail, e ulteriori applicativi e piattaforme di lavoro condiviso e collaborativo come Google Workspace for Education (ex G Suite for Education) con le app Classroom, Meet, Drive, Jamboard, Documenti, Presentazioni, Fogli e Moduli, che sono ampiamente utilizzati anche per facilitare e rendere più partecipata la didattica e la comunicazione a scuola. Infatti attraverso Classroom è possibile caricare materiale per gli alunni, proporre prove di verifica, riportare eventuali comunicazioni, proprio come un vero social network interno. É possibile visionare il Regolamento Dd'Istituto sull'utilizzo di tale piattaforma nella sezione dedicata del nostro sito web: https://www.icmirabellaeclano.edu.it/index.php/l-istituto/regolamenti Strumento ormai centrale a disposizione della scuola per la gestione di assenze, presenze, valutazioni e comunicazioni con le famiglie è il registro elettronico che permette di gestire la comunicazione con le famiglie e gestire gli incontri scuolafamiglia. Le famiglie

attraverso di esso possono visualizzare molte informazioni utili, interagendo con la scuola, su: andamento scolastico (assenze, argomenti lezioni e compiti, note disciplinari); risultati scolastici (voti, documenti di valutazione); udienze; eventi (agenda eventi); comunicazione varie.

---

# 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.

Si legge testualmente nell'Azione #6 del PNSD: " La scuola digitale, in collaborazione con le famiglie e gli enti locali, deve aprirsi al cosiddetto BYOD (Bring Your Own Device), ossia a politiche per cui l'utilizzo di dispositivi elettronici personali durante le attività didattiche sia possibile ed efficientemente integrato". L'attenzione verso le tecnologie digitali e il loro utilizzo in classe diventa così inclusivo e creativo, nel senso che le stesse vengono riproposte come strumenti da inserire nella didattica e nelle sperimentazioni laboratoriali. L'uso viene consentito, però, per scopi prettamente didattici, sotto il controllo e la responsabilità del docente che pianifica l'attività didattica. Come stabilito dall'autonomia scolastica, è nei nostri regolamenti d'Istituto che si inseriscono le sanzioni disciplinari in caso di uso scorretto dei cellulari da parte degli alunni e dei docenti, anche in vista di una eventuale apertura al BYOD per la scuola secondaria di I grado e per le classi 4 e 5 della scuola primaria. Si confida nella proficua collaborazione dei genitori con il nostro Istituto per educare i ragazzi ad un uso corretto e sicuro delle nuove tecnologie, per trasmettere valori quali il rispetto, la responsabilità e consapevolezza delle proprie azioni. Educare alla cittadinanza digitale è un dovere per il nostro Istituto. Formare i futuri cittadini della società della

conoscenza significa per noi educare alla partecipazione responsabile, all'uso critico delle tecnologie, alla consapevolezza e alla costruzione delle proprie competenze in un mondo sempre più connesso.

## *Il nostro piano d'azioni*

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

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 i genitori dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali

# 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.*

Per far sì che un intervento di sensibilizzazione sia efficace, è quindi importante fornire ai beneficiari informazioni chiare su quello che è lo stato attuale del tema che vogliamo trattare (ad es. se si vuol trattare il tema del Cyberbullismo, sarà opportuno fornire informazioni su quali sono le caratteristiche del fenomeno e i dati rappresentativi). In questo modo gli utenti avranno tutte le informazioni necessarie

per avere una fotografia chiara del contenuto che stiamo trattando e del perché è necessario impegnarsi verso un cambiamento (motivazione al cambiamento). Il problema della "sicurezza", tuttavia, è difficilmente riconducibile esclusivamente all'esistenza in sé di alcuni rischi, più o meno gravi e insidiosi, è necessario quindi che le migliori strategie di intervento siano di carattere prevalentemente preventivo. Il nostro Istituto, già impegnato su entrambi i fronti della sensibilizzazione e prevenzione, offre a studenti e docenti uno sportello di ascolto, tale servizio riesce a rispondere a tutte le richieste che giungono alla sua attenzione. Si propone, altresì, di continuare ad offrire agli studenti percorsi in grado di informarli e formarli riguardo al corretto utilizzo delle nuove tecnologie, affinchè essi siano in grado di dominare, e non di essere dominati, dai media.

---

# *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).

Un'indicazione operativa da tener presente per intervenire efficacemente è anche capire se si tratta effettivamente di cyberbullismo o di altra tipologia di comportamenti violenti o disfunzionali. Oltre al contesto, altri elementi utili ad effettuare questa valutazione sono le modalità in cui avvengono (alla presenza di un "pubblico"? Tra coetanei? In modo cronico e intenzionale? etc.) e l'età dei protagonisti. Un'altra indicazione operativa concerne una valutazione circa l'eventuale stato di disagio vissuto dalla/e persona/e minorenne/i coinvolta/e, per cui potrebbe essere necessario rivolgersi ad un servizio deputato ad offrire un supporto psicologico e/o di mediazione. Le strutture pubbliche a cui rivolgersi sono i servizi socio-sanitari del territorio di appartenenza. Per quanto riguarda la necessità di segnalazione e rimozione, 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 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. Parallelamente, nel caso in cui si ipotizzi che ci si possa trovare di fronte ad una fattispecie di reato (come, ad esempio, il furto di identità o la persistenza di una condotta persecutoria che mette seriamente a rischio il benessere psicofisico del bambino/a o adolescente coinvolto/a in qualità di vittima) si potrà far riferimento agli uffici preposti delle Forze di Polizia per inoltrare la segnalazione o denuncia/querela e permettere alle autorità competenti l'approfondimento della situazione da un punto di vista investigativo. Per un consiglio e un supporto è possibile, inoltre, rivolgersi alla Helpline di Telefono Azzurro per Generazioni Connesse: operatori esperti e preparati sono sempre a disposizione degli insegnanti, del Dirigente e degli operatori scolastici, oltre che dei/lle bambini/e, degli adolescenti, dei genitori e di altri adulti che a vario titolo necessitano di un confronto e di un aiuto per gestire nel modo più opportuno eventuali esperienze negative e/o problematiche inerenti l'utilizzo dei media digitali.

---

# *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.

Fermare l’odio sul web è possibile fin da giovanissimi, se già dalla scuola primaria si portano avanti delle azioni di contrasto a quello che viene definito “hate speech”. A tal fine,il nostro Istituto si propone di attivare percorsi che abbiano come obiettivi: 1. Far riflettere gli studenti sul linguaggio come strumento per negare o sostenere i diritti degli altri. 2. Far accrescere in ciascun allievo l’autostima e l’apprezzamento per l’unicità di ogni individuo. 3. Promuovere tra gli alunni la solidarietà, il rispetto, la capacità di “mettersi nei panni degli altri”. 4. Favorire la discussione e l’apprendimento cooperativo tra i discenti. 5. Stimolare nei ragazzi il pensiero critico.

---

# *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 tecnologia ha modificato gli ambienti che viviamo e ha un impatto sulla qualità della vita. La scuola può insegnare molto da questo punto di vista se integra la tecnologia nella didattica, mostrando un suo utilizzo funzionale che possa rendere più consapevoli i ragazzi e le ragazze delle proprie abitudini online. Per questo il nostro Istituto Comprensivo è intenzionato a promuovere percorsi sul benessere digitale, che mirino a responsabilizzare gli alunni nella: • gestione del tempo e dell'attenzione (gestire la frammentazione dell'attenzione, l'uso eccessivo degli schermi, il tempo in un ambiente iperstimolante); • comunicazione e collaborazione (comprensione delle dinamiche di relazione online, dei concetti di "identità digitale" e di "netiquette"); • ricerca e gestione delle informazioni (migliorare le competenze di ricerca, valutazione delle informazioni e verifica della validità delle fonti in rete); • creazione di contenuti online (produzione e pubblicazione di contenuti online, di qualsiasi natura, con particolare attenzione ai processi metacognitivi e auto-riflessivi legati al senso del contenuto che si vuole realizzare e diffondere, e ad alcuni aspetti legali, quali la privacy e il diritto d'autore)..

---

# *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.

I contenuti sessualmente espliciti, quindi, possono diventare materiale di ricatto assumendo la forma di "revenge porn" letteralmente "vendetta porno" fenomeno quest'ultimo che consiste nella diffusione illecita di immagini o di video contenenti riferimenti sessuali diretti al fine di ricattare l'altra parte (la Legge 19 luglio 2019 n. 69, all'articolo 10 ha introdotto in Italia il reato di revenge porn, con la denominazione di diffusione illecita di immagini o di video sessualmente espliciti). A livello preventivo, il nostro Istituto ritiene che sia importante attivare percorsi di informazione/formazione, ovviamente adeguati all'età e allo sviluppo psico-fisico, rivolti ai ragazzi della scuola secondaria di I grado, ai docenti e ai genitori per approfondire i rischi e le conseguenze di episodi di sexting.

---

# 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 miglior modo per prevenire casi di adescamento online è accompagnare ragazze e ragazzi in un percorso di educazione (anche digitale) all'affettività e alla sessualità. Ciò aiuterebbe a renderli più sicuri emotivamente e pronti ad affrontare eventuali situazioni a rischio, imparando innanzitutto a gestire le proprie emozioni, il rapporto con il proprio corpo e con gli altri. È molto importante, inoltre, che ragazzi e ragazze sappiano a chi rivolgersi in caso di problemi, anche quando pensano di aver fatto un errore, si vergognano o si sentono in colpa. Gli adulti coinvolti, genitori e docenti, devono essere un punto di riferimento per il minore che deve potersi fidare di loro e non sentirsi mai giudicato, ma compreso e ascoltato. Affinché ciò avvenga è necessario tenere sempre aperto un canale di comunicazione con loro sui temi dell'affettività, del digitale e perché no, della sessualità. La problematica dell'adescamento online (come quella del sexting), quindi, si inquadra in uno scenario più ampio di scarsa educazione emotiva, sessuale e di assenza di competenza digitale, in riferimento al modo in cui i/le ragazzi/e vivono la propria sessualità e la propria immagine online, al loro desiderio di esprimersi e affermare se stessi. La nostra scuola, quindi, intende portare avanti 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).

# 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.**

L'IC "R. Guarini" di Mirabella Eclano si propone di attuare programmi mirati alla presa di consapevolezza delle proprie sensazioni corporee, all'acquisizione di abilità di comportamento e al rafforzamento di abilità volte all'auto-protezione in rete. Tali percorsi potranno aiutare gli alunni a:

• riconoscere possibili situazioni di rischio, distinguendole da situazioni innocue.

• Reagire al potenziale abuso online tramite strategie assertive verbali e comportamentali. Riferire l'abuso a figure di riferimento di cui ci si fida.

• Rassicurarli nel caso in cui si senta responsabile o in colpa per quanto accaduto.

La nostra scuola intende, altresì, organizzare percorsi di educazione all'affettività, rivolti sia ad alunni della scuola primaria che secondaria, ovviamente adeguati all'età e allo sviluppo psico-fisico, orientati ad aiutare i bambini più grandi e gli adolescenti ad acquisire maggiore consapevolezza del proprio corpo e dei propri diritti in rete.

## *Il nostro piano d'azioni*

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

- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti agli/lle studenti/studentesse, con il coinvolgimento di esperti.

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

- Organizzare uno o più incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/lle studenti/studentesse.
- Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/lle studenti/studentesse.
- Organizzare uno o più eventi e/o dibattiti in momenti extrascolastici, sui temi della diversità e sull'inclusione rivolti a genitori, studenti/studentesse e personale della scuola.

# 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.

Per i ragazzi di oggi, nativi digitali, le interconnessioni tra vita e tecnologia sono la normalità. Essi, pur essendo spesso tecnicamente competenti, tendono a non cogliere le implicazioni dei loro comportamenti e tale fenomeno è tanto maggiore quanto è più forte il coinvolgimento emotivo nell'utilizzo dei nuovi media. Le tecnologie digitali offrono da tempo la possibilità di ampliare la propria rete di amicizie in modo quasi smisurato: non è infrequente che gli adolescenti "si sfidino" tra loro rispetto al numero di "amicizie" strette online. Avere molti amici nella vita virtuale, o molti followers, è elemento di grande popolarità e di vanto con gli amici della vita reale. Non a caso, quindi, gli adolescenti aggiungono tra le proprie cerchie, in particolare sui loro profili social, "amici di amici" senza valutare attentamente a chi stanno dando accesso alle proprie informazioni, alle proprie foto, spesso ai luoghi che frequentano, a quello che viene chiamato "diario virtuale". Tra le poche accortezze che molti ragazzi utilizzano per valutare l'affidabilità e la sicurezza di chi chiede loro di essere aggiunto tra gli amici, c'è quella di valutare il numero di amici in comune con la persona che aggiungono. Se per molti adulti sono evidenti l'ingenuità e l'imprudenza con cui bambini e adolescenti si approcciano a questa modalità di relazione e amicizia "online", per altri adulti e per i ragazzi stessi non è così. Questo li espone a rischi notevoli: tra gli altri, quello di condividere con sconosciuti l'accesso al loro mondo online, e quindi alle informazioni che potrebbero essere utilizzate in modo inaspettato e non sempre positivo. Aiutare i propri alunni a tutelarsi, scegliendo con cura chi frequentare online, è allora un compito importante anche dell'insegnante che contribuisce in questo modo alla loro tutela nella vita virtuale, con ripercussioni non banali nella vita reale. Tra i principali rischi, sia di carattere comportamentale che di matrice tecnica, ricordiamo:

- possibile esposizione a contenuti violenti e non adatti alla loro età;

- videogiochi diseducativi;

- pubblicità ingannevoli;

- accesso ad informazioni scorrette;

- virus informatici in grado di infettare computer e cellulari;

- possibili contatti con adulti che vogliono conoscere e avvicinare bambini/e o ragazzi/e (adescamento);

- rischio di molestie o maltrattamenti da coetanei(cyber-bullismo);

- scambio di materiale a sfondo sessuale(sexting);

- uso eccessivo di Internet/cellulare(dipendenza)

- adescamento on-line(grooming).

È opportuno che tutti i docenti del nostro Istituto, nell'espletamento delle proprie funzioni di formatori ed educatori sappiano cogliere ogni opportunità per riflettere insieme agli alunni su tali rischi. Fondamentale è monitorare costantemente le relazioni interne alla classe, onde individuare possibili situazioni di disagio ed intervenire tempestivamente, anche mediante il ricorso alle figure di sistema specializzate, per sostenere il singolo nelle situazioni di difficoltà personale e indirizzare il gruppo verso l'instaurazione di un clima positivo, di reciproca accettazione e rispetto, nelle situazioni di difficoltà socio-relazionale. Tale percorso interno potrà essere ulteriormente rinforzato dalla partecipazione a progetti e/o iniziative esterne coerenti con i temi sopra menzionati, cui il nostro istituto già ha sempre posto particolare attenzione e continuerà questo cammino selezionando iniziative significative promosse da Enti e/o Associazioni di comprovata affidabilità.

---

# *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.

La rilevazione dei casi problematici è compito dell'intera comunità educante, secondo la sensibilità di ciascuno e la presenza in particolari momenti o contesti. Perciò è fondamentale una corretta informazione/formazione e una sensibilizzazione di tutti gli adulti coinvolti. Il personale scolastico del nostro istituto, soprattutto nella componente docente, ma anche in quella del personale ATA, è invitato ad evitare atteggiamenti accusatori o intimidatori, in modo tale da riuscire a ricevere dai minori più fragili segnalazioni e confidenze circa situazioni problematiche vissute. E' fondamentale, infatti, osservare per tempo ciò che accade, per poter agire immediatamente nei confronti di atti non opportuni e in modo tale da poter scongiurare conseguenze a lungo termine ben più gravi, in quanto negative per il benessere e la crescita armonica dei minori coinvolti. La gestione dei casi rilevati andrà differenziata a seconda della loro gravità:

1. CASO A (sospetto) - è opportuno il coinvolgimento di tutti i docenti della classe per osservare e ricavare più informazioni possibili e soprattutto per prestare maggiore attenzione sulla vigilanza, soprattutto quando gli alunni si trovano nella sala informatica, poi occorre informare il Dirigente Scolastico e il Referente d'Istituto per il contrasto del bullismo e del cyberbullismo, al fine di valutare le possibili strategie d'intervento. Gli avvenimenti di lieve rilevanza possono essere affrontati e risolti con la discussione collettiva in classe. Altri casi ancora possono essere affrontati convocando genitori e alunno/a per riflettere insieme su quanto accaduto e individuare una strategia comune per affrontarlo e rimediare.E' bene sempre dialogare con la classe, ciò è utile per capire il livello di diffusione dell'episodio all'interno dell'Istituto. Per i casi più gravi bisogna informare il Dirigente Scolastico che nel caso di reati veri e propri effettuerà la denuncia all'autorità giudiziaria.

2. CASO B (evidenza) - il docente deve condividere immediatamente quanto osservato con tutti i docenti del team, con il Referente per il bullismo e il cyberbullismo, al fine di valutare insieme le possibili strategie di intervento. Si avvisa anche il Dirigente Scolastico che convoca il Consiglio di classe. Se non si ravvisano fattispecie di reato, è opportuno: informare i genitori (o chi esercita la responsabilità genitoriale) degli/delle

studenti/studentesse direttamente coinvolti/e (qualsiasi ruolo abbiano avuto), per strategie condivise e modalità di supporto; creare momenti di confronto costruttivo in classe, richiedere la rimozione, l'oscuramento o il blocco di contenuti offensivi ai gestori di siti internet o social (o successivamente, in caso di non risposta, al garante della Privacy). Per aiutare gli studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni il nostro istituto prevedere due strumenti di segnalazione:

1. una scatola per la raccolta di segnalazioni anonime da inserire in uno spazio accessibile e ben visibile dei vari plessi scolastici sia primaria che secondaria di primo grado.

2. Uno sportello di ascolto con professionisti.

---

# *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.

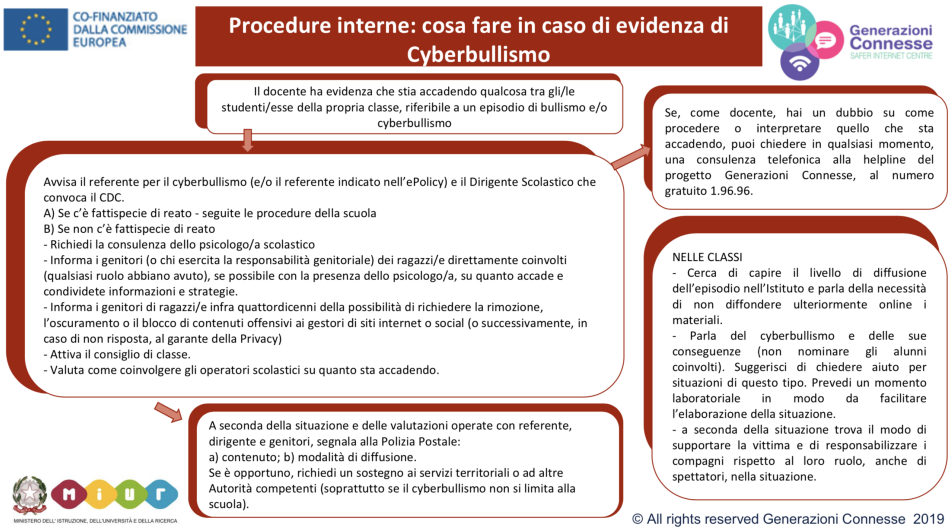
- **Aziende Sanitarie Locali**: forniscono supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in Rete. In alcune regioni, come il Lazio e la Lombardia, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da Internet e alle situazioni 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.

Il nostro istituto, per i casi più gravi, potrà contare su altre figure,enti, servizi presenti sul territorio, come sopra descritto, soprattutto quando la sistematicità e la gravità della situazione richiedono interventi più specifici che vanno oltre alle competenze della scuola. In caso di condotta incauta, scorretta o dell'abuso rilevate sui pc della scuola si provvederà a recuperare e conservare tutti i dati disponibili: la data e l'ora, il contenuto dei messaggi e l'ID del mittente o l'indirizzo web del profilo ed il suo contenuto. Circa i dispositivi personali ci si potrà assicurare che l'alunno vittima salvi nel suo telefono ogni messaggio, voce/testo/immagine, conservando così il numero del mittente. Conservare la prova è utile per far conoscere l'accaduto, in base alla gravità, ai genitori degli alunni, al Dirigente scolastico ed eventualmente denunciare alla Polizia Postale.

---

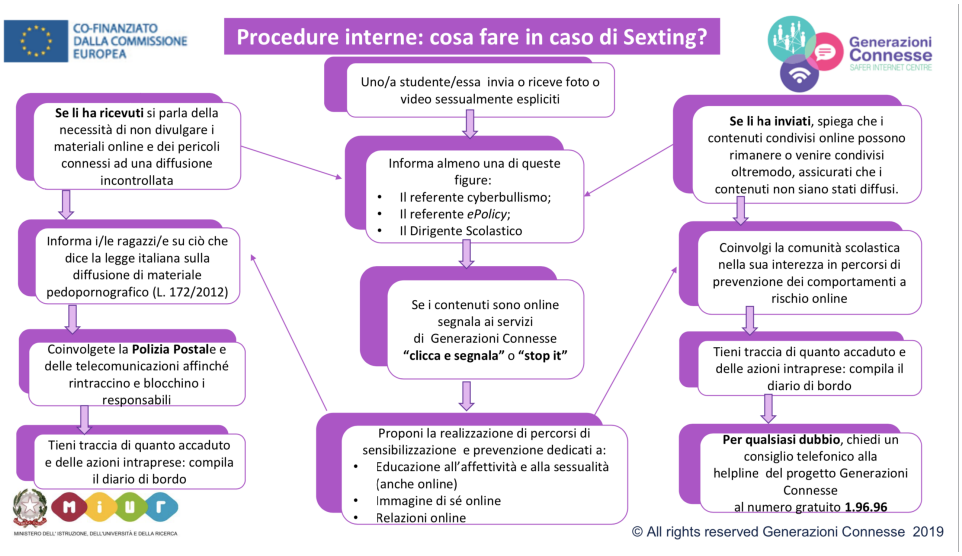
# *5.4. - Allegati con le procedure*

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

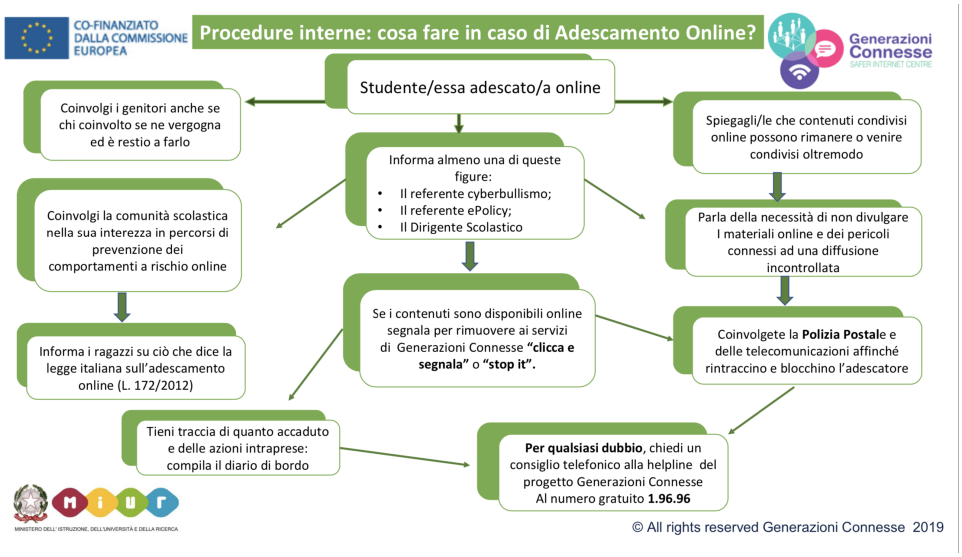




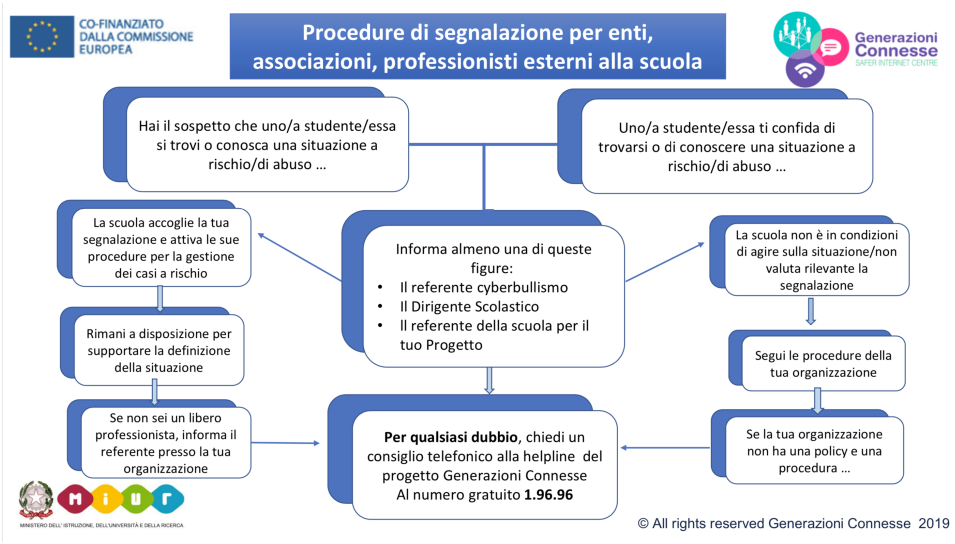
# Procedure interne: cosa fare in caso di sexting?




## 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

Non è prevista nessuna azione

## *Il nostro piano d'azioni*

Schede per la rilevazione dei casi e delle procedure attuate dal nostro Istituto:

ALLEGATO A - Prima segnalazione dei casi di (presunto) bullismo e vittimizzazione

ALLEGATO B - Valutazione approfondita dei casi di bullismo e vittimizzazione

ALLEGATO C - Scheda di monitoraggio