# Documento di ePolicy

SAIS01300N

MARCO TULLIO CICERONE

VIA MATTEOTTI - 84036 - SALA CONSILINA - SALERNO (SA)

Antonella Vairo

# 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.

## *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.

Riflessione sui ruoli e sulle responsabilità di ciascuna figura del mondo scuola

Affinché l'ePolicy 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.

N**el seguente documento vengono definiti con chiarezza ruoli, compiti e responsabilità** di ciascuna delle figure all'interno dell'Istituto.

A seguire alcuni spunti e consigli per una riflessione sui ruoli e sulle responsabilità di ciascuna figura del mondo scuola:

# Il Dirigente Scolastico

- garantisce la sicurezza, anche online, di tutti i membri della comunità scolastica;

- promuove la cultura della sicurezza online e contribuisce a organizzare, insieme al docente referente sulle tematiche del bullismo/cyberbullismo corsi di formazione specifici per tutte le figure scolastiche sull' utilizzo positivo e responsabile delle TIC;

- ha la responsabilità di gestire ed intervenire nei casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali.

# La funzione strumentale Cyberbullismo:

- opera al fine di prevenire e contrastare il cyberbullismo ;

- stabilisce contatti con le forze di polizia, con associazioni e centri di aggregazione giovanile impegnati nel contrasto e nella prevenzione del cyberbullismo;

- organizza incontri di formazione per docenti, student e genitori;

- informa i docenti su incontri di formazione organizzati da terzi;

- organizza azioni di monitoraggio;

- redige l'epolicy dell'Istituto, con la collaborazione della commissione Generazioni connesse;

- coopera con il docente referente per lo sviluppo dell'insegnamento di Cittadinanza e costituzione all'interno dell'Istituto, al fine di rendere gli studenti cittadini consapevoli anche nella dimensione del digitale;

- coordina la commissione Generazioni connesse.

## La commissione Generazioni connesse:

- riflette sull'impiego consapevole delle TIC all'interno della comunità scolastica;

- affianca il referente per il contrasto al cyberbullismo nelle sue funzioni, in particolare: * nella revisione periodica dell'epolicy e nel monitoraggio sulla sua effettiva applicazione;

* nel coinvolgimento della comunità scolastica in iniziative di formazione e di sensibilizzazione sul corretto impiego delle TIC;

- segue corsi di formazine e di aggiornamento utili alla stesura e alla revisione del documento di epolicy.

## L'animatore digitale e il team digitale:

- supporta il personale scolastico da un punto di vista non solo tecnico-informatico, ma anche in riferimento ai rischi online, alla protezione e gestione dei dati personali;

- promuove percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale". Il referente per bullismo e cyberbullismo:

- coordina e promuove iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo, anche avvalendosi di figure, istituzione e collaborazioni extrascolastiche;

- coinvolge, con progetti e percorsi formativi ad hoc, studenti, colleghi e genitori.

## I docenti:

- si impegnano a diffondere la cultura dell'uso responsabile delle TIC e della Rete, anche integrandole nell'insegnamento delle loro discipline;

- provvedono alla propria formazione/al proprio aggiornamento sull'utilizzo del digitale

Il personale tecnico e amministrativo e ausiliario:

- deve essere coinvolto nella segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo e nel raccogliere, verificare e valutare le informazioni inerenti possibili casi di bullismo/cyberbullismo.

# Gli studenti e le studentesse:

- si impegnano a utilizzare al meglio le tecnologie digitali in coerenza con quanto richiesto dai docenti e a partecipare attivamente a progetti ed attività che riguardano l'uso positivo delle TIC proposti dalla scuola.

# I genitori:

- promuovono un uso consapevole delle TIC e della Rete e un impiego responsabile dei device personali;

- collaborano coi docenti nella segnalazione di eventuali abusi.

Dato questo quadro normativo, rispetto ad un profilo prettamente processuale anche in materia di bullismo e cyberbullismo (dunque non in via esclusiva), si può parlare di **tre tipologie di "culpa":**

- **culpa in vigilando:** concerne la mancata sorveglianza attiva da parte del docente responsabile verso il minore (cosi come da art. 2048 del c.c.). Tale condizione è superabile se ci si avvale di una prova liberatoria di non aver potuto impedire il fatto (recita il terzo comma dell'art. 2048 c.c.: "le persone indicate nei commi precedenti sono liberate dalla responsabilità soltanto se provano di non aver potuto impedire il fatto").
- **culpa in organizzando:** si riferisce ai provvedimenti previsti e presi dal Dirigente Scolastico ritenuti come non soddisfacenti e quindi elemento favorevole al verificarsi dell'eventuale incidente.
- **culpa in educando:** fa capo ai genitori i quali hanno instaurato una relazione educativa con il/la figlio/a, ritenuta come non adeguata, insufficiente o comunque carente tale da metterlo/a nella situazione di poter recare danno a terzi.

---

## *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).

Affinché tutti i soggetti esterni che erogano attività in ambito scolastico siano sensibilizzati e resi consapevoli dei rischi online che possono correre gli studenti e le studentesse e dei comportamenti corretti che devono adottare a scuola, sarà predisposta un'informativa sintetica sull'ePolicy comprensiva delle procedure di segnalazione, da condividere con tutti gli operatori.

Tale condivisione garantirà una più efficace e corretta collaborazione tra scuola ed enti esterni e una maggiore sicurezza degli studenti coinvolti.

---

# *1.4 - Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica*

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

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

- la pubblicazione del documento sul sito istituzionale della scuola;

- il Patto di Corresponsabilità, che deve essere sottoscritto dalle famiglie e rilasciato alle stesse all'inizio dell'anno scolastico;

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

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

La condivisione del documento di Policy con tutta la comunità educante ha precise finalità educative e organizzative, infatti:

- condividere e comunicare il documento agli studenti e alle studentesse significa dare loro una base di partenza per un uso consapevole e maturo dei dispositivi e della tecnologia informatica; dare loro regole condivise di sicurezza circa il comportamento da tenere a scuola e nei contesti extrascolastici; dare loro elementi per poter riconoscere e quindi prevenire comportamenti a rischio sia personali che dei/delle propri/e compagni/e. condividere e comunicare il documento al personale scolastico permette di orientare tutte le figure sui temi in oggetto, a partire da un uso corretto dei dispositivi e della Rete in linea anche con il codice di comportamento dei pubblici dipendenti;

- condividere e comunicare il documento ai genitori sul sito istituzionale della scuola, nonché tramite momenti di formazione specifici e durante gli incontri scuola-famiglia migliora la consapevolezza e il coinvolgimento degli stessi nel processo di educazione all'uso dei media dei loro figli.

In considerazione dell'età dei nostri studenti (13-19) e del buon livello di familiarizzazione di tutta la comunità scolastica con strumenti digitali, sito web dell'Istituto e app nativa, il canale di comunicazione e condivisione più adatto per l'E-policy è certamente un'area dedicata del sito istituzionale, ma saranno necessari momenti assembleari (anche on line per fasce di età o gruppi di appartenenza) per la promozione del documento, con la attiva partecipazione di tutte le componenti del mondo della scuola.

---

# *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 responsabilità di stabilire azioni educativo e comminare sanzioni è attribuita ai singoli consigli di classe che stabiliranno caso per caso come meglio intervenire, in relazione alla situazione specifica e in base alla loro conoscenza dei soggetti coinvolti.

In particolare, le sanzioni/azioni educative che potranno essere comminate a seconda dei casi sono:

- richiamo verbale;

- sanzioni commisurate alla gravità della violazione commessa (tra cui anche assegnazione di attività aggiuntive da svolgere su temi di Cittadinanza e costituzione);

- convocazione dei genitori o tutori per un colloquio con gli insegnanti;

- convocazione dei genitori o tutori per un colloquio col Dirigente scolastico.

Per le infrazioni riguardanti cyberbullismo saranno trattate in conformità con la legge.

Sono da considerarsi atti di cyberbullismo:

- **la condivisione online di immagini o video di compagni/e in pose umilianti o denigratorie;**
- **la condivisione di scatti intimi e/o a sfondo sessuale;**
- **l'invio di immagini volto all'esclusione di compagni/e.**

Valutata la natura e la gravità dell'accaduto potrebbe rendersi necessario denunciare l'episodio alle **Forze dell'Ordine** e/o garantire supporto psicologico allo/a studente/ssa attraverso i servizi predisposti.

---

# *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.

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.

L'Istituto Marco Tullio Cicerone si impegna ad aggiornare entro l'a.s. 2021/2022 il Regolamento dell'Istituto Scolastico con specifici riferimenti all'E-policy, così come anche il Patto di Corresponsabilità e lo Statuto degli studenti e delle studentesse, in coerenza con le Linee Guida MIUR e le indicazioni normative generali sui temi in oggetto.

---

# *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.

Si monitoreranno, ad esempio:

- l'avanzamento del piano d'azioni programmate a breve, medio e lungo termine; - la tipologia e quantità di interventi messi in atto per promuovere le competenze digitali e l'uso delle TIC nei percorsi educativi e didattici;

- la tipologia e quantità degli interventi messi in atto per la prevenzione e gestioni dei rischi online etc;

- la tipologia e quantità degli interventi messi in atto per formare il corpo docente all' utilizzo consapevole e sicuro di Internet e delle tecnologie digitali e incrementarne le competenze digitali - la tipologia e quantità degli interventi messi in atto per informare i genitori sull'importanza dell'educazione alla cittadinanza digitale;

- la partecipazione delle diverse componenti della scuola agli interventi programmati.

Il Gruppo di lavoro per la ePolicy d'Istituto, costituito su nomina del Dirigente scolastico, provvederà annualmente alla revisione o all'aggiornamento del documento.

---

## *Il nostro piano d'azioni*

**L'istituto Marco Tullio Cicerone si**

## impegna a svolgere, entro un'annualità scolastica, le seguenti azioni:

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

## Azioni da svolgere nei prossimi 3 anni:

- 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.

Nella progettazione del curricolo digitale si farà riferimento in particolare ai seguenti documenti:

- Piano Nazionale Scuola Digitale
- DigComp 2.1
- Raccomandazione del Consiglio europeo relativa alle competenze chiave per l'apprendimento permanente (C189/9, p. 9).

**Competenze da promuovere:**

- "Alfabetizzazione e dati"
- Comunicazione e Collaborazione
- Sicurezza

I percorsi garantiscono, alla fine del ciclo scolastico, un'alfabetizzazione digitale

completa e consapevole degli studenti del nostro Istituto.

---

# 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.

Infatti, per accompagnare studenti e studentesse nel loro percorso, gli insegnanti devono avere e/o raggiungere un buon livello di formazione in merito all'utilizzo e l'integrazione delle TIC nella didattica.

Devono saper procedere disinvoltamente, partendo da compiti semplici (es.: individuare i fabbisogni informativi; trovare dati, informazioni e contenuti attraverso una semplice ricerca in ambienti digitale etc.) per arrivare ai compiti complessi che presentano molti fattori di interazione (ad es.: creare nuove app o piattaforme per navigare, ricercare e filtrare portali e offerte).

È su tali premesse che l'Istituto, nel Piano per la formazione del personale a, ha considerato come prioritaria tale esigenza formativa e favorisce la partecipazione del personale ad iniziative promosse sia direttamente dalla scuola (ad es. con l'aiuto dell'animatore digitale), sia liberamente scelte dai docenti ("Pedagogia Digitale"), purché coerenti con il piano di formazione e con gli obiettivi di miglioramento che l'Istituto si è dato per il triennio 19-22, in particolare nell'ambito "Pedagogia Digitale 2020/2021" per Incrementare le competenze digitali del personale grazie all'attivazione di percorsi di formazione/aggiornamento/autoformazione in sinergia con l'animatore digitale e i docenti più esperti, anche attraverso l'utilizzo delle risorse online e la condivisione di buone pratiche e documenti condivisi (cfr. aggiornamento PtOF 2019/22, PTOF Cicerone Sala Consilina). Tali corsi prevedono approfondimenti sull'uso del registro elettronico, delle piattaforme per l'apprendimento a distanza, della Lim, di altro software applicativo, con particolare riferimento all'inclusione degli alunni con BES.

## 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.

I docenti dell'Istituto saranno invitati a seguire percorsi formativi adeguati che abbiano come oggetto l'uso responsabile della rete. Infatti gli studenti, per la loro giovane età, comunicano ed esprimono se stessi attraverso dispositivi tecnologici e i docenti necessitano di strumenti per poter guidare ed educare i ragazzi nei comportamenti online.

Un primo passo già realizzato quest'anno è stato quello di individuare le nuove esigenze formative dettate dall'introduzione del nuovo insegnamento della Educazione Civica (macroarea Cittadinanza digitale) e, in generale, dalla gestione della classe in tempi di Didattica Digitale.

Per offrire ai docenti riferimenti utili all'autoformazione sono stati proposti: la navigazione del sito "Generazioni connesse" per i percorsi formativi gratuiti online.

Per approfondimenti sulla didattica digitale ai tempi del Covid e per alcune indicazioni e videoconferenze utili a favorire l'inclusione nella didattica digitale e aiutare gli allievi a vivere al meglio l'uso della Rete è stato proposto anche il corso online gratuito "Pedagogia Digitale"

## 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.

Al seguente link è possibile consultare tutte le attività, le iniziative proposte dal nostro istituto, i riferimenti per un uso responsabile e consapevole degli strumenti digitali e i contatti per il supporto o eventuali segnalazioni:

https://www.istitutocicerone.edu.it/

## *Il nostro piano d'azioni*

### AZIONI (sviluppate nell'arco dell'anno scolastico 2019/2020)

- analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.
- analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica (corso "Pedagogia Digitale").
- analisi del fabbisogno formativo del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali (iscrizione alla piattaforma "Generazioni Connesse").
- coinvolto una rappresentanza dei genitori per individuare i temi di maggiore interesse nell'ambito dell'educazione alla cittadinanza digitale.
- incontri con psicologo per i docenti/genitori/alunni/ATA.

### AZIONI (da sviluppare nell'arco dei tre

## anni scolastici successivi)

- coinvolgere una rappresentanza dei genitori per individuare i temi di maggiore interesse nell'ambito dell'educazione alla cittadinanza digitale;
- organizzare altri incontri con esperti per i docenti sulle competenze digitali;
- continuare gli incontri con esperti psicologi per il supporto di genitori/alunni/docenti/ATA.

# 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.

La scuola sta adeguando progressivamente tutti i sistemi informatici e amministrativi/gestionali relativi al tema della privacy (trattamento, protezione, informazione) e tutte le procedure relative a garantire il diritto alla riservatezza, in linea con la recente normativa europea e nazionale.

Sono state individuate le figure del titolare del trattamento, il responsabile del trattamento e il responsabile della protezione dei dati. Per una più rapida e visibile comunicazione di questa materia alla comunità scolastica, l'istituto ha raccolto e pubblicherà tutta la documentazione sul proprio sito ufficiale nell'albo consultabile online al seguente indirizzo: https://www.trasparenzascuole.it/Public/APDPublic_ExtV2.aspx?CF=83002040653

Per i processi di dematerializzazione della gestione amministrativo/contabile, in coerenza con il CAD e per la realizzazione del Piano triennale dell'offerta formativa aggiornato dal piano della didattica digitale integrata, la scuola utilizza diverse piattaforme online.

A seguito della raccomandazione del M.I., nelle modalità della didattica a distanza, si utilizza la piattaforma Gsuite di Google (https://www.google.it/) con i diversi applicativi forniti di videoconferenza, di chat, di classi virtuali. Tale scelta è stata realizzata per gli alti livelli di garanzia offerti in tema di sicurezza, di privacy e di consenso informato da parte del gestore del servizio.

La scuola ha registrato ogni alunno ed ogni docente con un account identificativo che ne permette il riconoscimento anche a distanza.

Un'altra piattaforma utilizzata dalla scuola per la didattica e per la gestione amministrativa e contabile è quella offerta dalla società Axios (Axios).

In particolare, sono utilizzati i servizi del registro elettronico, l'anagrafe degli studenti, l'archivio e la gestione elettronica dei documenti nel rispetto del Codice dell'amministrazione digitale. Anche per gli applicativi Axios sono garantiti alti standard di conservazione e protezione dei dati. Inoltre la scuola opera, soprattutto per i servizi amministrativi, sulla piattaforma SIDI, implementata dal Ministero dell'Istruzione per l'interscambio di dati e informazioni tra l'amministrazione centrale e la scuola. La scuola ha un proprio sito ufficiale il cui dominio .edu.it rientra tra quelli offerti dal Ministero (https://www.istitutocicerone.edu.it/). Il referente del sito è un assistente tecnico.

In generale, come vuole il Regolamento europeo circa l'obbligo di adozione di misure

tecniche e organizzative da parte del titolare del trattamento, tutte le suddette misure tecniche adottate e realizzate da aziende terze rispettano il principio di privacy by design e privacy by default. Tutte le piattaforme utilizzate sono implementate con sistemi di protocollo sicuri HTTPS e permettono il backup in cloud dei dati trattati. La scuola non è in possesso di un sistema di videosorveglianza dei locali interni all'edificio, né di aree esterne specifiche, quella degli accessi alle aree di parcheggio e delle aree esterne.

---

# *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, divisa su tre plessi, è dotata di accesso a internet con rete di fibra-rame (max 100Mb/s) per quanto riguarda la rete interna alla scuola in uno specifico plesso mentre tutte le classi sono cablate con rete lan a Gbit e wifi mentre in un altro plesso vi è la stessa fornitura di fibra ma la rete studenti è solo wifi, nel terzo plesso fornitura con rete wifi e poche classi cablate con rete lan. Per entrambe le sedi la scuola si è dotata di un'offerta di connettività di rete a banda larga per poter andare incontro alla domanda di connettività delle attività didattiche e amministrative. Per queste ultime, i servizi amministrativi, per lo più concentrati in un unico plesso, possono contare su una rete LAN separata da quella dedicata alle attività didattiche. Per le attività didattiche la connettività resta non ancora pienamente sufficiente per soddisfare l'accesso contemporaneo di 50 classi di media più 8 laboratori e 3 palestre. L'Istituto si è dotato di un doppio canale di accesso alla rete per entrambe le sedi (Lan e wireless). L'accesso via cavo, presente nella quasi totalità degli ambienti scolastici, permette alle aule di essere ognuna un punto di accesso indipendente alla rete. L'accesso wi-fi anche è possibile da tutti gli ambienti scolastici ma solo per tecnici e docenti.

Non in tutte le aule vi è la LIM ma laddove presente è collegata via cavo ad Internet. L'accesso al pc della classe è differenziato tra un amministratore di sistema, che si occupa della manutenzione e degli aggiornamenti, e un account guest che è rivolto ai docenti della classe.

La scuola implementerà il Regolamento per la Didattica Digitale con alcune norme specifiche sul corretto uso delle TIC e della Rete, di cui si propongono di seguito alcuni principi-guida.

Rispetto all'uso di Internet, gli studenti dovranno impegnarsi a:

- utilizzare la rete nel modo corretto;

- segnalare immediatamente materiali inadeguati ai propri insegnanti;

- durante le attività che prevedono lo smartphone, utilizzarlo esclusivamente per svolgere le attività didattiche previste;

- tenere spento lo smartphone al di fuori delle attività didattiche che ne prevedano l'utilizzo non utilizzare unità rimovibili personali senza autorizzazione;

- non scaricare materiali e software senza autorizzazione;

I docenti dovranno impegnarsi a:

- utilizzare la rete nel modo corretto

- monitorare l'uso che gli studenti fanno delle tecnologie a scuola

- formare gli studenti all'uso della rete

- non utilizzare devices personali se non per uso didattico.

Il patto educativo di corresponsabilità è stato aggiornato recependo la dimensione degli ambienti digitali come nuovo spazio di relazione educativa: infatti il documento ha indicato tra l'elenco degli impegni dei soggetti coinvolti anche i nuovi diritti e doveri delle varie componenti della comunità educante.

Quest'anno, come anticipato nel § 2.1, il percorso si è arricchito e potenziato incrociandosi con la macroarea di Cittadinanza digitale nell'ambito dell'insegnamento dell'Educazione civica. Ciò ha permesso di estendere la formazione anche al primo biennio e di estenderla anche ai temi della Internet Security and Safety.

Per quanto riguarda la formazione alle competenze digitali rivolta agli studenti la scuola sta attivando percorsi per le competenze trasversali e per l'orientamento nella proposta di formazione e certificazione delle competenze digitali attraverso progetti PON.

---

## *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.

La scuola è dotata di strumenti di comunicazione online interni ed esterni. In particolare si è cercato di investire su pochi ma solidi canali di comunicazione che garantissero l'unione tra la dimensione orizzontale e interattiva con quella della privacy e della protezione, anche per evitare un'eccessiva esposizione della comunità a fenomeni di iper-connessione. Il principale canale di comunicazione esterna è il sito istituzionale della scuola, anche con la sua versione in app su smartphone. In particolare, il sito adempie alla duplice funzione di albo/vetrina e portale di accesso ad altre sezioni specifiche dell'attività scolastiche. Un altro canale di comunicazione esterno è la pagina della scuola nel contenitore ministeriale di Scuola in chiaro, strumento utilizzato in modo particolare come vetrina nelle attività di orientamento in entrata. Anche il portale di Amministrazione trasparente ha questa funzione ma con il

taglio specifico amministrativo, gestionale e contabile. In sintesi, si può dire che la comunicazione esterna della scuola si attesti prioritariamente sulla dimensione informativa.

Il principale canale di comunicazione interna è il registro elettronico, con tutte le sue classiche funzioni. In esso interagisce la dimensione amministrativa con quella didattica, la componente genitoriale e studentesca con quella docente e dell'amministrazione.

Un altro canale interno è quello della messaggistica via posta elettronica che arricchisce la comunicazione istituzionale con una serie di strumenti di supporto alle attività scolastiche. Ancora, il portale del progetto Comitato Studentesco Itis, dedicato alle attività di recupero in itinere, fa incontrare la domanda individualizzata degli studenti di recupero di argomenti durante il corso dell'anno con l'offerta di lezioni di supporto e di chiarimento da parte del team dei docenti coinvolti.

Una menzione a parte riguarda il contenitore di applicativi di comunicazione sia interna che esterna, adottato dalla scuola per la didattica digitale integrata, che è il pacchetto di GSuite di Google, in particolare per le app Gmail, Meet e Classroom che permettono una comunicazione online anche in streaming tra gli utenti del dominio.

---

# *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.

La scuola ha favorito e regolamentato la pratica del Byod (Bring your own device) nelle

attività didattiche per varie ragioni, tra cui superare il divario di accesso alla rete e far intervenire tutti mediante un proprio dispositivo a causa della insufficienza di device individuali a disposizione della scuola. Tuttavia si è data anche un piano di intervento di acquisto di strumentazione tecnologica mediante i bandi europei, soprattutto per rispondere al bisogno di alcune famiglie che necessitavano di un supporto, in modo particolare durante il periodo della didattica a distanza.

In linea di principio la scuola accoglie il seguente decalogo del Miur per l'uso dei dispositivi mobili BYOD a scuola:

1. Ogni novità comporta cambiamenti. Ogni cambiamento deve servire per migliorare l'apprendimento e il benessere delle studentesse e degli studenti e più in generale dell'intera comunità scolastica

2. I cambiamenti non vanno rifiutati, ma compresi e utilizzati per il raggiungimento dei propri scopi. Bisogna insegnare a usare bene e integrare nella didattica quotidiana i dispositivi, anche attraverso una loro regolamentazione. Proibire l'uso dei dispositivi a scuola non è la soluzione.

3. La scuola promuove le condizioni strutturali per l'uso delle tecnologie digitali. Fornisce, per quanto possibile, i necessari servizi e l'indispensabile connettività, favorendo un uso responsabile dei dispositivi personali (BYOD). Le tecnologie digitali sono uno dei modi per sostenere il rinnovamento della scuola.

4. La scuola accoglie e promuove lo sviluppo del digitale nella didattica. La presenza delle tecnologie digitali costituisce una sfida e un'opportunità per la didattica e per la cultura scolastica. Dirigenti e insegnanti attivi in questi campi sono il motore dell'innovazione. Occorre coinvolgere l'intera comunità scolastica anche attraverso la formazione e lo sviluppo professionale.

5. I dispositivi devono essere un mezzo, non un fine. È la didattica che guida l'uso competente e responsabile dei dispositivi. Non basta sviluppare le abilità tecniche, ma occorre sostenere lo sviluppo di una capacità critica e creativa.

6. L'uso dei dispositivi promuove l'autonomia delle studentesse e degli studenti. È in atto una graduale transizione verso situazioni di apprendimento che valorizzano lo spirito d'iniziativa e la responsabilità di studentesse e gli studenti. Bisogna sostenere un approccio consapevole al digitale nonché la capacità d'uso critico delle fonti di informazione, anche in vista di un apprendimento lungo tutto l'arco della vita.

7. Il digitale nella didattica è una scelta: sta ai docenti introdurla e condurla in classe. L'uso dei dispositivi in aula, siano essi analogici o digitali, è promosso dai docenti, nei modi e nei tempi che ritengono più opportuni.

8. Il digitale trasforma gli ambienti di apprendimento. Le possibilità di apprendere sono ampliate, sia per la frequentazione di ambienti digitali e condivisi, sia per l'accesso alle informazioni, e grazie alla connessione continua con la classe. Occorre

regolamentare le modalità e i tempi dell'uso e del non uso, anche per imparare a riconoscere e a mantenere separate le dimensioni del privato e del pubblico.

9. Rafforzare la comunità scolastica e l'alleanza educativa con le famiglie. È necessario che l'alleanza educativa tra scuola e famiglia si estenda alle questioni relative all'uso dei dispositivi personali. Le tecnologie digitali devono essere funzionali a questa collaborazione. Lo scopo condiviso è promuovere la crescita di cittadini autonomi e responsabili.

10. Educare alla cittadinanza digitale è un dovere per la scuola. Formare i futuri cittadini della società della conoscenza significa 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 il personale adulto dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

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

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli
- studenti e delle studentesse
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte dei docenti

# 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.*

## 4.2 - Cyberbullismo: che cos'è e come prevenirlo

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

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

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

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

Il sistema scolastico deve prevedere azioni preventive ed educative e non solo sanzionatorie.

Con gli allievi sarà necessario condurre una attenta disamina delle diverse tipologie di cyberbullismo possibili; ad esempio:

- Attacchi scritto-verbali: si tratta di comportamenti verbali o scritti volti ad offendere la vittima, ad es. commenti offensivi sui social network

- Esclusione: si esclude qualcuno dai gruppi on line come ad esempio quelli su

Whatsapp - Impersonificazione: indica l'accesso non autorizzato e l'uso delle credenziali private, dell'account di un/a compagno/a

- Attacchi visuali: comprendono l'invio o la condivisione, pubblica e/o privata, di foto o video personali, compromettenti o imbarazzanti In particolare, sarà opportuno far riflettere gli alunni sui tratti distintivi di questo fenomeno, quali:

1) La pervasività o assenza di limiti spazio-temporali: la diffusione di materiale tramite Internet è incontrollabile e non è possibile prevederne i limiti. Un contenuto offensivo e denigratorio online può, quindi, diventare virale e distruggere in alcuni casi la reputazione della vittima che non ha più spazi-rifugio. Spegnere il cellulare o il computer non basta, così come cancellare tutti i propri profili social. Il solo pensiero che eventuali contenuti denigratori continuino a diffondersi online è doloroso e si accompagna ad un senso costante di rabbia e impotenza. L'attacco può avvenire ad ogni ora del giorno e della notte.

2) La convinzione dell'anonimato: chi offende online potrebbe tentare di rimanere nascosto dietro un nickname. Sentendosi protetti dall'anonimato ci si sente liberi e più forti nel compiere atti denigratori, senza il timore di essere scoperti. Tuttavia, quello dell'anonimato è un "falso mito della Rete" perché ogni nostra azione online è rintracciabile e riconducibile a noi con gli strumenti opportuni o con l'intervento della Polizia Postale. L'anonimato del cyberbullo, inoltre, è anche uno dei fattori che stanno alla base del forte stress percepito dalla vittima.

3) L'indebolimento dell'empatia: i neuroni specchio, che ci permettono di "leggere" gli altri che abbiamo di fronte, di capirli e di provare emozioni simili a quelle che loro provano, non si attivano quando le interazioni avvengono prevalentemente online. La riduzione di empatia che ne consegue può degenerare nei comportamenti noti messi in atto dai cyberbulli.

4) Il feedback non tangibile: il cyberbullo non vede in modo diretto le reazioni della vittima e, ancora una volta, ciò riduce fortemente l'empatia e il riconoscimento del danno provocato. L'impossibilità di vedere con i propri occhi l'eventuale sofferenza e umiliazione provata dalla vittima fa sì che il tutto venga percepito come "uno scherzo" divertente a cui partecipare, di cui ridere o a cui essere indifferenti. Inoltre, il cyberbullismo non lascia segni fisici evidenti sulla vittima e si consuma in un contesto virtuale che spesso viene percepito dai ragazzi come non "reale", come un mondo ludico a sé stante. Per questo il fenomeno viene talvolta sottovalutato anche dal mondo adulto, familiare e scolastico.

La mediazione tecnologica, infatti, porta ad un certo distanziamento fra aggressore e vittima, causando quello che Bandura ha definito come "disimpegno morale" con la conseguente minimizzazione delle responsabilità individuali. Tale fenomeno vale non solo per il cyberbullo, ma anche per i cosiddetti bystanders, ossia coloro che sono spettatori dei fatti. Sarà molto importante sottolineare nell'azione educativa come il cyberbullismo non sia una problematica che riguarda unicamente vittima e cyberbullo,

bensì di gruppo: Il gruppo “silente”, che partecipa senza assumersi la responsabilità, rappresenta anche l’elemento che può fermare una situazione di cyberbullismo e questo, appunto, costituisce un gancio educativo. Il sistema scolastico deve a riguardo prevedere azioni preventive ed educative e non solo sanzionatorie.

Pertanto il nostro Istituto adotterà in primis l’approccio della prevenzione universale, che prevede quattro passi:

1) Promozione della consapevolezza degli studenti sul fenomeno del bullismo e cyberbullismo

2) Somministrazione del Questionario dei ruoli dei partecipanti (QRP), che sarà restituito in forma anonima, o del Questionario self-report (nel primo viene chiesto ai partecipanti di nominare i compagni che mettono in atto il comportamento descritto in 6 items che definiscono i sei ruoli dei partecipanti; nel secondo viene fatta una valutazione di quante volte lo studente si è trovato a fare e/o ricevere atti di bullismo in un determinato periodo di tempo)

3) Coinvolgimento degli spettatori, che si articola in:

a. sensibilizzazione del gruppo classe attraverso un modulo sulla consapevolezza emotiva dei ragazzi che favorisca l’empatia, intesa sia come capacità di comprendere le emozioni proprie e altrui che come capacità di sentire le stesse emozioni dell’altro. L’obiettivo è quello di analizzare alcune emozioni chiave legate al vissuto della (cyber-vittima), stimolando un’attivazione empatica sia una riflessione condivisa sull’empatia stessa.

b. promozione di strategie di coping: capita che, pur riconoscendo di trovarsi davanti ad una situazione di bullismo, non si intervenga. I motivi possono riferirsi ad aree diverse: non assumersi la responsabilità; temere le conseguenze; valutazione del proprio intervento come inefficace; essere un pro-bullo. Una discussione, oppure situazioni di role-playing possono aiutare a capire “che cosa si può fare” in base alle proprie caratteristiche personali e alla situazione specifica: prendersi cura della vittima; adottare comportamenti pro-vittima; adottare comportamenti anti-bullo sono le possibili strategie da mettere in atto quando ci si trova ad essere spettatori in una situazione di (cyber)bullismo. In modo trasversale, un comportamento di coping positivo è: il cercare aiuto, chiedere ad un adulto, segnalare

4) Metodi di promozione del contributo attivo degli adolescenti, come:

a. la peer education modalità utilizzata per facilitare un cambiamento positivo nei comportamenti del proprio gruppo di riferimento. Essa implica la formazione dei ragazzi attraverso il potenziamento delle abilità sociali,-si basa sull’insegnamento della tecnica dell’ascolto attivo, la promozione dell’empatia, la stimolazione del problem-solving e delle life skills;

b. il peer supporting è una modalità che può prevedere la realizzazione di uno

"sportello amico" da parte di un gruppo di peer educators per una durata di alcune settimane. Allo sportello si presentano a rotazione due peer educators, affiancati dallo psicologo, che si occupa della supervisione, del supporto e del monitoraggio. Durante gli incontri possono presentarsi, per es., studenti delle classi prime a due/tre persone alla volta. Alla fine di ogni incontro lo psicologo definisce un momento di debriefing e riflessione finale con i peer educators coinvolti.

Per la gestione dei casi di bullismo e vittimizzazione, il nostro istituto adotterà il seguente protocollo di intervento:

1) Valutazione dell'episodio da parte dei docenti Referenti per il Bullismo e il Cyberbullismo attraverso colloqui volti ad accertare la tipologia e la gravità dei fatti (attraverso, ad esempio le Florence bullying and victimization Scales che valutano il livello di sofferenza della vittima e il livello di rischio del bullo).

2) Intervento con la classe quando è coinvolta nell'accaduto (compagno/a del gruppo w.a. della classe); quando il livello di sofferenza della vittima e di gravità del problema non è molto elevato; quando in classe ci sono persone di cui la vittima si fida.

3) Intervento individualizzato con il bullo, attraverso colloqui responsabilizzanti e riparativi, se il caso in oggetto è considerato come bullismo sistematico.

4) Intervento individualizzato con la vittima per rielaborare l'esperienza ed attivare un supporto mirato a potenziare le proprie abilità sociali (essere più assertivi ed esercitare il diritto ad essere rispettati, incrementare il senso di fiducia in sé e nelle proprie capacità a costruire relazioni positive…) attraverso la tecnica del roleplay e il modellamento dell'assertività.

5) Intervento in rete con il territorio: nel caso in cui gli atti subiti siano di notevole gravità per cui la sofferenza della vittima sia molto elevata, oppure il bullo sia a rischio di sviluppare condizioni psichiatriche, i Referenti per il Bullismo e il Cyberbullismo contattano i servizi sociali. Lo scopo è quello di aiutare la vittima a sviluppare strategie di coping per fronteggiare le situazioni stressanti e aumentare nel bullo la consapevolezza dei propri comportamenti.

---

## *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.

La prima azione suggerita riguarda incontri di sensibilizzazione con le classi al fine di aumentare la consapevolezza del fenomeno. Tali incontri si focalizzeranno sullo smontaggio di alcune convinzioni che potrebbero risultare fuorvianti, quali:

- non esistono gli hater come sottocategoria della popolazione. Esistono persone normali che, occasionalmente, magari si esprimono in maniera dissennata.

- non esiste un numero definito di “parole d’odio”, vietando le quali si risolve il problema. Non si può “vietare l’odio”. Lo si può segnalare al gestore della piattaforma sulla quale ci troviamo, lo si può, in alcuni casi, perseguire legalmente o sanzionare, ma è impossibile vietarlo.

- l’odio è diventato più pubblico, e forse viene esibito con meno remore, dato che online è possibile incontrare molte persone che la pensano allo stesso modo, rafforzando reciprocamente perfino opinioni che prima erano tenute più nascoste. Non bisogna colpevolizzare i social in sé quanto il modo in cui essi vengono utilizzati.

- anche se gli episodi di incitamento all’odio sui social sembrano tantissimi, numericamente sono inferiori alle interazioni pacifiche, solo che il discorso pubblico indugia su di loro.

Il percorso di sensibilizzazione si focalizzerà successivamente sulle competenze necessarie per vivere nella dimensione di iper-connessione. Gli studenti, pertanto, saranno sollecitati a lavorare su se stessi attraverso:

- il prestare attenzione ai post che si scrivono o che si ricondividono e alle affermazioni che si fanno poiché le parole in rete sono “nude” (non hanno l’ausilio del nostro corpo) e quindi maggiormente fraintendibili.

- l’esercitarsi ad entrare in relazione con gli altri. L’uso di video e le tecniche di role

playing possono aiutare a modellare le forme della comunicazione quotidiana per evitare di alimentare scambi verbali ostili.

- l'esercitare il dubbio rispetto a ciò che si legge, spesso scritto appositamente per provocare una reazione istintiva;

- l' imparare a decodificare meglio il mondo che ci circonda e a parlarne in modo più riflesso.

- il tener presente che le parole scritte sono quasi immortali, pubbliche quindi incontrollabili, sia come numero di lettori sia come possibile passaggio da un canale all'altro e dall'online all'offline.

Il nostro Istituto si attiverà sulla formazione degli studenti attraverso il potenziamento delle loro abilità comunicative sulle quali si può fondare una successiva competenza sociale. Il training ed il coinvolgimento di insegnanti nel progetto sulle competenze comunicative diventano importanti per la buona riuscita del progetto stesso. Gli insegnanti saranno introdotti alla conoscenza dei siti che in Rete propongono materiale didattico atto a diffondere consapevolezza sull'uso del linguaggio e che utilizzeranno all'interno delle proprie discipline.

---

# *4.4 - Dipendenza da Internet e gioco online*

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

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

La Dipendenza da Internet, che può manifestarsi anche attraverso le ore trascorse online a giocare, rappresenta una questione importante per la comunità scolastica che deve attenzionare il fenomeno e fornire gli strumenti agli studenti e alle studentesse affinché questi siano consapevoli dei rischi che comporta l'iperconnessione.

La Società Italiana Intervento Patologie Compulsive definisce la dipendenza da Internet come progressivo e totale assorbimento del soggetto alla Rete;

di seguito alcune caratteristiche specifiche:

- Dominanza. L'attività domina i pensieri ed il comportamento del soggetto, assumendo

un valore primario tra tutti gli interessi.

- Ricaduta. Tendenza a ricominciare l'attività dopo averla interrotta.

- Conflitto. Conflitti inter-personali tra il soggetto e coloro che gli sono vicini, conflitti intra-personali interni a se stesso, a causa del comportamento dipendente.

- Alterazioni del tono dell'umore. L'inizio dell'attività provoca cambiamenti nel tono dell'umore. Il soggetto prova un aumento d'eccitazione o maggiore rilassatezza come diretta conseguenza dell'incontro con l'oggetto della dipendenza. La condizione di dipendenza da Internet e dal gioco online ha ripercussioni sulla sfera delle relazioni interpersonali che diventano via via più povere e alle quali si preferisce il mondo virtuale, con alterazioni dell'umore e della percezione del tempo.

I docenti, nell'ambito dell'insegnamento di Educazione civica (macroarea Cittadinanza digitale) faranno formazione e indicheranno strategie per un uso più consapevole delle tecnologie volte a favorire il "benessere digitale", cioè la capacità di creare e mantenere una relazione sana con la tecnologia attraverso:

- la ricerca di equilibrio nelle relazioni anche online

- la capacità di gestire il sovraccarico informativo e le distrazioni (ad esempio, le notifiche) la capacità di interagire negli ambienti digitali in modo sicuro e responsabile

- l'uso degli strumenti digitali per il raggiungimento di obiettivi personali.

Si dedicheranno momenti specifici a riflettere con studenti e studentesse per fare in modo che la tecnologia sia strumento per raggiungere i propri obiettivi e non sia solo fonte di distrazione o addirittura di ostacolo. Ad esempio, durante le lezioni di educazione civica si potrebbe provvedere alla distribuzione iniziale di questionari esplorativi che portino i ragazzi a focalizzarsi su questioni quali:

"Come trascorri il tempo on line?";

"Quando aggiunge valore alla tua vita e quando ti fa perdere tempo?";

"Quale atteggiamento potrei cambiare quando sono online?";

"Che ruolo ha e deve avere la tecnologia (internet o il gioco) nella mia vita?".

Allo stesso modo, qualora emergesse il tema dell'uso dei videogiochi, essi dovranno essere ripensati non in termini negativi ma di benessere digitale, costituendo ormai una parte non piccola del mondo di studenti e studentesse.

Quindi si rifletterà insieme a ragazzi e ragazze attraverso domande tipo:

"Quando i videogiochi sono una risorsa?";

"A quali tipi di contenuti accedi con maggiore frequenza?"

“A che ora e per quanto tempo usate i videogiochi?”

Diventa utile riflettere in termini di qualità e tempo. La visione di video tratti da siti quali Generazioni Connesse sui temi della dipendenza da internet può costituire, inoltre, un ulteriore momento di confronto tra pari e con i docenti per riflettere sulle modalità d'uso e di approccio alla Rete Infine, si suggerisce ai docenti di strutturare regole condivise e stipulare con gli studenti una sorta di “patto” d’aula, proponendo anche delle alternative metodologiche e didattiche valide che abbiano come strumento giochi virtuali d’aula (Es. adoperando la LIM o il dispositivo personale).

Inoltre, attraverso la costante e quotidiana integrazione della tecnologia nella didattica, la scuola stessa mostra un suo utilizzo funzionale, costituendo così un affiancamento molto prezioso in questo processo di consapevolezza. L’approccio dell’Istituto sarà, quindi, quello di non demonizzare la tecnologia o il gioco, ma di cercare di entrare nel mondo degli/lle studenti e delle studentesse, stabilendo chiare e semplici regole di utilizzo.

---

# *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.

Indipendentemente dalla relazione di partenza in cui sono generati, le immagini o i video sessualmente espliciti, diffusi attraverso il cellulare, possono poi essere condivisi, all’insaputa del mittente, attraverso siti, e-mail, chat, con una cerchia macroscopicamente diversa dalle intenzioni originarie. Questi materiali, una volta diffusi in Rete, possono dar luogo a forme di “revenge porn”, reato che indica la condivisione illecita di materiali sessualmente espliciti per ricattare un soggetto, minorenne o maggiorenne, ed è punito dalla legge 69/2019 del Codice penale.

I danni legati a questo fenomeno riguardano aspetti emotivo-relazionali perché minano la fiducia alla base della condivisione intenzionale e aspetti eminentemente legati alle TIC, ovvero la pervasività con cui si diffondono i contenuti in Rete e la persistenza del fenomeno stesso che rende, potenzialmente, impossibile il controllo della rimozione definitiva di un materiale immesso in Internet, dato che può essere scaricato su altri dispositivi e inoltrato su piattaforme diverse anche in momenti successivi. I rischi più gravi, legati al revenge porn, riguardano violenza sessuale e psicologica, adescamento online, umiliazione, bullismo, cyberbullismo, molestie e stress emotivo che generano

fenomeni di disagio psicofisico variabili, riconducibili all'area depressiva che sfociano nei casi più estremi -come purtroppo la cronaca registra- in episodi suicidiari.

Se con la legge 69/2019 che introduce il reato di "revenge porn" e l'articolo 612 ter del Codice penale derubricato si affrontano le conseguenze giudiziarie di questo fenomeno che coinvolge in prima linea la Polizia postale, in ambito scolastico saranno promosse:

-la possibilità di affrontare tematiche legate al sexting in incontri tematici mirati, coordinati da un Referente del gruppo di Lavoro Generazioni connesse;

-l'introduzione di questionari di autovalutazione, all'interno di gruppi classe specifici, volti ad attivare interventi di prevenzione selettivi;

- la formazione di studenti del triennio o di ex studenti volontari che partecipino alle discussioni guidate secondo lo schema educativo peer to peer;

-la pubblicizzazione della linea d'ascolto 1.96.96 e la chat del Telefono Azzurro (www.azzurro.it/sostegno).

---

# *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.

Data la natura del fenomeno, rivolto ad entrambi i generi e basato su una dinamica subdola, apparentemente lontana dalla violenza ma basata su un'attenzione che asseconda quel bisogno tipico dell'età adolescenziale di sentirsi riconosciuti e apprezzati, bisogna precisare in primo luogo un aspetto. Molto spesso negli adescamenti online, i minori comunicano con interlocutori che sfruttano una falsa identità, di genere e/o anagrafica, il che ci mette di fronte ad un elemento di attenzione ulteriore: una buona parte degli adolescenti scambia messaggi o avvia conversazioni in chat con sconosciuti, talvolta condividendo immagini intime.

È importante segnalare che, dopo la ratifica della Convenzione di Lanzarote del 2012, in Italia è punito il reato di adescamento online anche quando non avviene nessun incontro tra le parti. Il processo di adescamento online segue un iter graduale che si può così sintetizzare:

- Fase dell'amicizia iniziale: serve all'adescatore a conquistare la fiducia del minore, sondarne gli interessi, stabilire un contatto via via più profondo fino ad affrontare argomenti sempre più personali.

- Fase di risk assessment: serve all'adescatore a comprendere e valutare le abitudini e i rischi legati all'approccio con la potenziale vittima (tipi di dispositivi in uso, controllo da parte degli adulti, abitudini di navigazione e tempo di utilizzo dei devices, ambienti in cui la connessione avviene), se possibile, in questa fase, l'adescatore ottiene il numero privato del/la minore.

- Fase della costruzione del rapporto di fiducia: ad un progressivo aumento della confidenza stabilita tra adescatore e vittima possono seguire regali (anche di piccolo conto) e attenzioni, volte a consolidare la fiducia e si possono verificare i primi scambi di immagini (non necessariamente a sfondo sessuale).

- Fase dell'esclusività: la confidenza raggiunta viene "blindata" con un patto sempre più rigido in cui il rapporto si consolida attraverso richieste di segretezza e codici che tendono ad isolare il/la minore dalla rete di relazioni consuete, familiari e amicali. In questa fase spesso compaiono ricatti morali che fanno leva su timori, ansie, sensi di colpa, minacce vere e proprie.

- Fase della relazione sessualizzata: si fa insistente la richiesta di immagini a sfondo erotico e di incontri offline. Nel caso lo scambio di foto o video sia già avvenuto l'adescatore potrebbe minacciare di diffonderli in rete e, d'altra parte, provare a "normalizzare" la relazione descrivendola come perfettamente naturale.

Di seguito alcuni aspetti del comportamento o delle attitudini dei minori che possono rientrare nel novero di quei segnali che è opportuno guardare con attenzione in ambito scolastico:

- le conoscenze sessuali del/la minore sembrano inappropriate alla sua età;

- si manifesta un progressivo isolamento e l'unico ambiente interessante per il/la

minore sembra quello digitale;

- si verificano frequenti allusioni alla reputazione di un/una studente/essa con prese in giro o allusioni ripetute

- si viene informati, sommariamente e con imbarazzo, dell'esistenza di immagini o video online riguardanti un/a minore.

Data la sempre maggiore precocità con cui gli adolescenti entrano in possesso di smartphone o altri devices che permettono loro l'accesso autonomo alla Rete, in ambito scolastico sembra efficace promuovere:

1) corsi di educazione sessuale e all'affettività, promossi da team di esperti, sessuologi, psicologi, educatori (www.scuola.net progetto "Domande Scomode @ School");

2) incontri informativi aperti alle famiglie sui rischi connessi alla navigazione;

3) corsi di educazione digitale con particolare attenzione ai temi della privacy, della tutela dei dati e dell'identità online;

4) l'ascolto e la comunicazione, in famiglia e a scuola, relativamente a temi strettamente connessi alla crescita sana degli adolescenti, quali la sessualità, la parità di genere, il rispetto per sé e per gli altri.

Nel caso in cui, in ambito scolastico si venga a conoscenza di un caso di adescamento online è bene ricordare che: - chiunque ne venga a conoscenza deve immediatamente segnalare il sospetto alla Polizia postale;

- è sconsigliato sostituirsi al minore nei contatti con l'adescatore;

- è opportuno che i devices in uso al minore restino nelle sue disponibilità per non compromettere eventuali prove del reato;

- Generazioni connesse offre una apposita Helpline (1.96.96) per supportare in modo adeguato il/la minore.

---

# *4.7 - Pedopornografia*

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

**La legge n. 269 del 3 agosto 1998** *"Norme contro lo sfruttamento della*

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

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

In un'ottica di attività preventive, il tema della pedopornografia è estremamente delicato, occorre parlarne sempre in considerazione della maturità, della fascia d'età e selezionando il tipo di informazioni che si possono condividere.

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

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

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

La pedopornografia, purtroppo, è nata prima di Internet e si manifesta anche in modo autonomo rispetto al mezzo informatico, detto questo siamo tutti consapevoli dell'enorme estensione di raggio che la Rete ha offerto a questo genere di attività, aumentando i canali virtuali di comunicazione, scambio e traffici di materiale pedopornografico.

L'aumento della potenza della rete Internet consente la circolazione e la diffusione di

video e immagini in pochi secondi e le tecnologie dei devices personali permettono la produzione di materiale home made, pronto per essere condiviso e diffuso. Le statistiche confermano il legame che lega questo tipo di materiali con gli abusi pedopornografici ed è per questo che bisogna vigilare con molta attenzione sui segnali che possano denunciare fenomeni di questo tipo.

Pertanto, in ambito scolastico si promuoveranno:

1) adeguate campagne informative sulla pedopornografia;

2) corsi di educazione alle relazioni e all'affettività;

3) una rete d'ascolto di facilitatori adulti- anche tra gli insegnanti- a disposizione degli studenti e delle studentesse;

4) la sensibilizzazione delle famiglie con incontri dedicati.

## *Il nostro piano d'azioni*

**AZIONI (da sviluppare nell'arco dell'anno scolastico 2021/2022).**

□ Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse.

□ 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.

□ Promuovere incontri e laboratori per studenti e studentesse dedicati all' Educazione Civica Digitale.

□ 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 (www.scuola.net progetto "Domande Scomode @ School").

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

□ Organizzare uno o più eventi e/o dibattiti in momenti extra-scolastici, sui temi della diversità e sull'inclusione rivolti a genitori, studenti/studentesse e personale della scuola.

□ Pianificare e realizzare progetti di peer-education - sui temi della sicurezza online - nella 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.

# 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.

## 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.

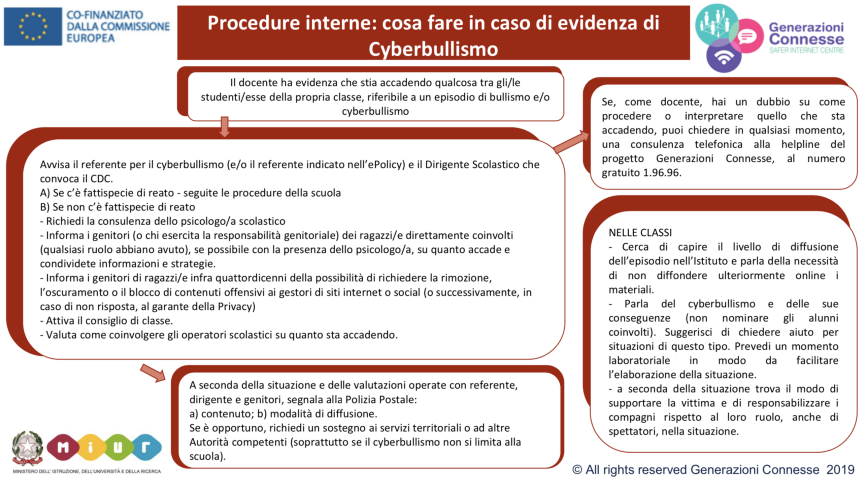
A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all'utilizzo di Internet può presentare.

- **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.

# *5.4. - Allegati con le procedure*

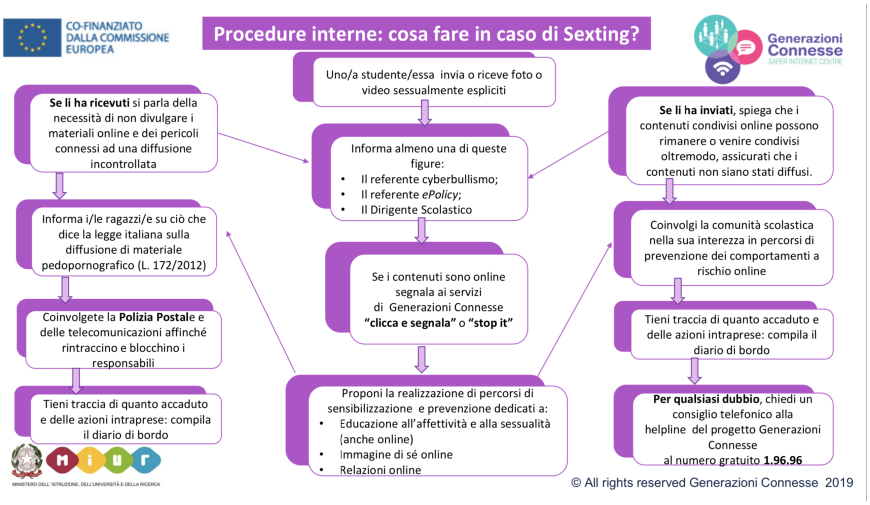
## Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



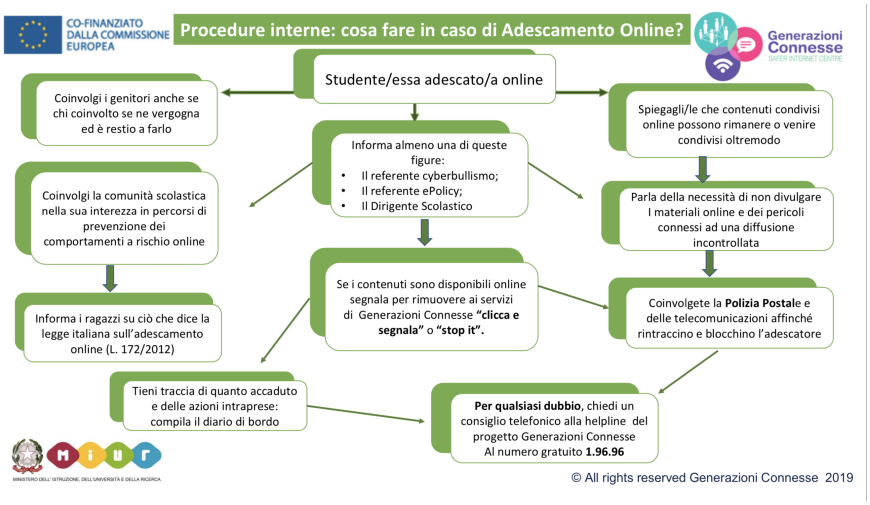


---

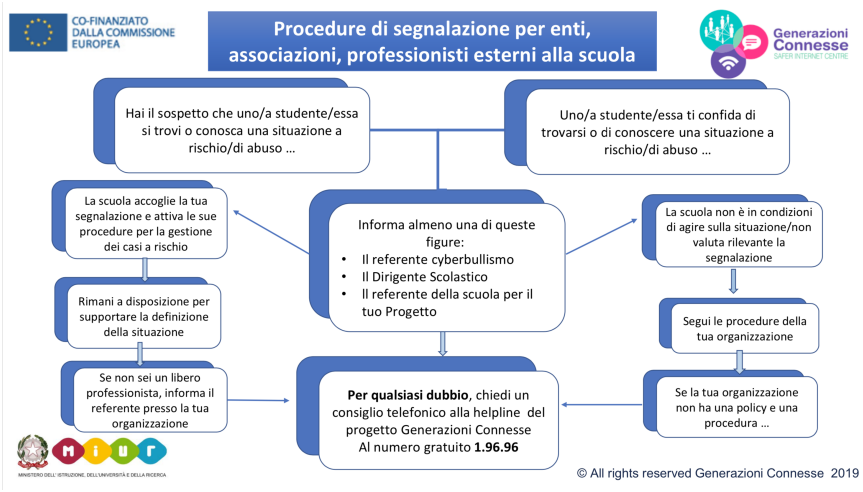
## Procedure interne: cosa fare in caso di sexting?




## 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

## *Il nostro piano d'azioni*