



# Documento di ePolicy

---

CZIS00900L

IS "GIOVANNA DE NOBILI" CATANZARO

VIA PIAVE 1 - 88100 - CATANZARO - CATANZARO (CZ)

ANGELO GAGLIARDI

# 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

### 1. Presentazione dell'ePolicy

1. Scopo dell'ePolicy
2. Ruoli e responsabilità
3. Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto
4. Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica
5. Gestione delle infrazioni alla ePolicy
6. Integrazione dell'ePolicy con regolamenti esistenti
7. Monitoraggio dell'implementazione dell'ePolicy e suo aggiornamento

### 2. Formazione e curriculum

1. Curriculum sulle competenze digitali per gli studenti
2. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica
3. Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali
4. Sensibilizzazione delle famiglie e Patto di corresponsabilità

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

1. Protezione dei dati personali
2. Accesso ad Internet
3. Strumenti di comunicazione online
4. Strumentazione personale

### 4. Rischi on line: conoscere, prevenire e rilevare

1. Sensibilizzazione e prevenzione
2. Cyberbullismo: che cos'è e come prevenirlo
3. Hate speech: che cos'è e come prevenirlo
4. Dipendenza da Internet e gioco online
5. Sexting
6. Adescamento online
7. Pedopornografia

### 5. Segnalazione e gestione dei casi

1. Cosa segnalare
2. Come segnalare: quali strumenti e a chi
3. Gli attori sul territorio per intervenire
4. Allegati con le procedure

## Perché è importante dotarsi di una E-policy?

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

all'uso di Internet.

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

L'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 attivare azioni formative ed educative mirate, in raccordo con la legge n.71/ 2017 "Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo".

Al contempo, con il presente documento redatto in continuità con il progetto MIUR "Generazioni Connesse", e con la collaborazione del Safer internet Centre, il nostro Liceo vuole garantire una formazione trasversale a tutti gli attori scolastici, nella consapevolezza e con volontà di attivare un sistema metodologico ed educativo, condiviso con gli alunni , le loro famiglie e le altre agenzie di socializzazione operanti sul territorio, che sappia:

1. Promuovere l'educazione al rispetto, attraverso l'assunzione di un approccio formativo e regolamentativo basato sul riconoscimento dei diritti umani e sulla tutela della dignità personale e sociale, su un dialogo paritario e rispettoso tra tutti gli individui, che promuova il contrasto a messaggi di odio, violenza e discriminazione sia online che offline;
2. Sviluppare un pensiero critico per un uso consapevole delle tecnologie digitali e della capacità di assumersi la responsabilità delle proprie azioni e delle proprie scelte nell'utilizzo delle tecnologie digitali;
3. Promuovere l'Educazione all' informazione, finalizzata alla capacità di valutare provenienza, qualità e credibilità delle fonti informative e di giudicare la qualità e la completezza delle informazioni raccolte.

---

## ***1.2 - Ruoli e responsabilità***

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

### **Il Dirigente Scolastico**

Il Dirigente Scolastico deve garantire la sicurezza, anche online, di tutti i membri della

comunità scolastica, promuove la cultura della sicurezza online e ha la responsabilità di gestire ed intervenire nei casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali.

### **L'Animatore digitale**

L'Animatore digitale può supportare 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, oltre che essere uno dei promotori di percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale" (con riferimento, ad esempio, allo sviluppo delle competenze digitali previste anche nell'ambito dell'educazione civica); può monitorare e rilevare eventuali episodi o problematiche connesse all'uso delle TIC a scuola, e avere il compito di controllare che gli utenti autorizzati accedano alla Rete della scuola con apposita password, per scopi istituzionali e consentiti (istruzione e formazione).

### **Il Referente bullismo e cyberbullismo**

Il referente bullismo e cyberbullismo ha il compito di coordinare e promuovere iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo. A tal fine, può avvalersi della collaborazione delle Forze di polizia, delle associazioni e dei centri di aggregazione giovanile del territorio. Fondamentale, dunque, il suo ruolo non solo in ambito scolastico ma anche in quello extrascolastico, per il coinvolgimento di studenti, colleghi e genitori.

### **Il consiglio di istituto**

Il consiglio di istituto approva ed adotta il Regolamento per la prevenzione e il contrasto al Bullismo e Cyberbullismo. Qualora a scuola si verificassero azioni di bullismo e/o casi di diffusione a terzi di foto/audio/video in violazione delle norme sulla privacy, si pronuncia se esistono gli estremi - previa verifica della sussistenza di elementi concreti e precisi dai quali si evinca la responsabilità disciplinare dello studente - sulle sanzioni che prevedono l'allontanamento dalla comunità scolastica per un periodo superiore ai 15 giorni.

### **Il collegio dei docenti**

Il collegio dei docenti promuove scelte didattiche ed educative, anche in collaborazione con altre scuole in rete, per la prevenzione del fenomeno del bullismo e cyberbullismo; prevede all'interno del PTOF corsi di aggiornamento e formazione in materia di Cittadinanza digitale e di prevenzione dei fenomeni di bullismo e cyberbullismo, rivolti al personale docente ed Ata; coinvolge, nella prevenzione e contrasto al fenomeno del bullismo e del cyberbullismo, tutte le componenti della comunità scolastica, particolarmente quelle che operano nell'area dell'informatica, partendo dall'utilizzo sicuro di Internet a scuola promuove sistematicamente azioni di sensibilizzazione dei fenomeni del bullismo e cyberbullismo sul territorio in rete con enti, associazioni, istituzioni locali ed altre scuole, coinvolgendo alunni, docenti,

genitori ed esperti

### **I Docenti**

I Docenti hanno un ruolo centrale nel diffondere la cultura dell'uso responsabile delle TIC e della Rete. Possono integrare parti del curriculum della propria disciplina con approfondimenti ad hoc, promuovendo anche l'uso delle tecnologie digitali nella didattica. I docenti accompagnano e supportano gli studenti nelle attività di apprendimento e nei laboratori che prevedono l'uso della LIM o di altri dispositivi tecnologici che si connettono alla Rete; hanno il dovere morale e professionale di segnalare al Dirigente Scolastico qualunque problematica, violazione o abuso, anche online, che vede coinvolti gli studenti.

### **Il personale Amministrativo, Tecnico e Ausiliario (ATA)**

Il personale ATA si occupa, ciascuno per la propria funzione, del funzionamento dell'Istituto scolastico che passa anche attraverso lo sviluppo della cultura digitale e dell'organizzazione del tempo scuola. Deve quindi essere concretamente coinvolto (v. L.107/15) nelle attività di formazione e autoformazione in tema di bullismo e cyberbullismo e soprattutto nella segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo.

### **Gli Studenti**

Gli Studenti devono utilizzare al meglio le tecnologie digitali in coerenza con quanto richiesto dai docenti; con il supporto della scuola dovrebbero imparare a tutelarsi online e a tutelare i propri compagni e rispettarli.

### **I Genitori**

I Genitori sono i primi responsabili sull'uso responsabile e consapevole dei device personali; devono anche essere partecipi e attivi in continuità con l'Istituto scolastico nelle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete; dovrebbero relazionarsi in modo costruttivo con i docenti sulle linee educative che riguardano le TIC e la Rete e comunicare con loro circa i problemi rilevati quando i propri figli non usano responsabilmente le tecnologie digitali o Internet. È estremamente importante che accettino e condividano quanto scritto nell'ePolicy dell'Istituto.

### **Gli Enti educativi esterni e le associazioni**

Gli Enti educativi esterni e le associazioni che entrano in relazione con la scuola devono conformarsi alla politica della stessa riguardo all'uso consapevole della Rete e delle TIC e promuovere comportamenti sicuri, la sicurezza online e assicurare la protezione degli studenti durante le attività che si svolgono insieme. Si ricorda che, anche in materia di bullismo e cyberbullismo, si può parlare di tre tipologie di "culpa":

1. *Culpa in vigilando*: concerne la mancata sorveglianza attiva da parte del

docente responsabile verso il minore (così 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").

2. *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.
3. *Culpa in educando*: fa capo ai genitori i quali hanno instaurato una relazione educativa con il figlio, ritenuta come non adeguata, insufficiente o comunque carente tale da metterlo 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).

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.

---

## ***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/le studenti/esse) si faccia a sua volta promotore del documento.

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

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

Il documento è approvato dal Collegio dei Docenti e dal Consiglio di Istituto 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.

Ordinariamente i coordinatori di classe provvedono alla diffusione del documento di ePolicy tramite la piattaforma Classroom adottata dal nostro istituto.

Le famiglie riceveranno il documento via mail o tramite pubblicazione sul sito scolastico nell'area "Regolamenti"

---

## ***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.

**MANCANZE DISCIPLINARI** Tutte le infrazioni andranno tempestivamente segnalate al Dirigente Scolastico, che avrà cura di convocare le parti interessate onde valutare le possibili azioni da intraprendere. La Scuola prenderà e manterrà nel tempo tutte le precauzioni necessarie e adatte per garantire agli studenti l'accesso a materiale e ambienti appropriati. La scuola non può in ogni caso farsi carico della responsabilità derivante dal materiale furtivamente trovato su internet o per eventuali conseguenze causate dall'accesso ad internet. I Referenti per il bullismo e il suo team sono coloro ai quali bisogna rivolgersi immediatamente nel caso in cui si verificano incidenti o comportamenti dubbi. Qualsiasi sospetto, rischio, violazione va segnalato in giornata ai suddetti Referenti, che riferiscono al Dirigente.

Al personale, agli studenti e agli altri componenti della comunità scolastica sono date informazioni sulle infrazioni previste e le eventuali sanzioni. Le sanzioni, riferite soprattutto agli alunni, avranno come carattere preferenziale quello educativo/riabilitativo e in ogni caso verrà coinvolta la componente genitori, in qualità di primi educatori. All'interno del Regolamento d'Istituto si trovano invece le diverse sanzioni, graduate in modo proporzionale rispetto all'entità delle varie forme di bullismo. È fondamentale per l'Istituto, anche nella sanzione, creare sempre occasioni di recupero. Risulta infatti possibile commutare i giorni di sospensione con attività socialmente utili alla comunità scolastica o alle associazioni convenzionate.

**MANCANZE DISCIPLINARI NEL CASO DI ATTI DI BULLISMO O CYBERBULLISMO** Sono da considerarsi tipologie persecutorie qualificate come BULLISMO:

- la violenza fisica, psicologica o l'intimidazione del gruppo, specie se reiterata;
- l'intenzione di nuocere;
- l'isolamento della vittima.

Rientrano nel CYBERBULLISMO:

- FLAMING: litigi on line nei quali si fa uso di un linguaggio violento e volgare
- HARASSMENT: molestie attuate attraverso l'invio ripetuto di messaggi offensivi
- CYBERSTALKING: invio ripetuto di messaggi contenenti esplicite minacce fisiche o fortemente intimidatori, al punto che la vittima arriva a temere per la propria incolumità
- DENIGRAZIONE: pubblicazione all'interno di comunità virtuali di pettegolezzi, commenti denigratori, dicerie crudeli o foto compromettenti per danneggiare la reputazione della vittima
- EXPOSURE: pubblicazione on line di segreti, informazioni private e/o imbarazzanti su un'altra persona
- IMPERSONIFICAZIONE: sostituzione di persona con l'obiettivo di inviare

messaggi ingiuriosi che screditano la vittima; violazione dell'account di qualcuno per farsi passare per questa persona ed inviare messaggi per dare una cattiva immagine della stessa e danneggiarne la reputazione

- **ESCLUSIONE**: escludere deliberatamente una persona da un gruppo on line (come una lista di amici) per ferirla
- **SEXTING**: invio di messaggi corredati da immagini a sfondo sessuale

**SANZIONI DISCIPLINARI - CONTRAVVENZIONI** L'Istituto considera, come infrazione grave, i comportamenti, accertati, che si configurano come forme di bullismo e cyberbullismo e li sanziona sulla base di quanto previsto nel Regolamento d'Istituto. Gli episodi di bullismo e cyberbullismo saranno sanzionati, privilegiando sanzioni disciplinari di tipo riparativo, convertibili in attività a favore della comunità scolastica. Il Dirigente scolastico, in caso di constatato episodio di cyberbullismo, contatterà, comunque, la polizia postale che potrà indagare e rimuovere, su autorizzazione dell'autorità giudiziaria, i contenuti offensivi ed illegali e cancellare l'account del cyberbullo che non rispetta le regole di comportamento. Le possibili infrazioni del personale docente sono così di seguito schematizzate:

1. utilizzo delle tecnologie della scuola, d'uso comune con gli alunni, non connesso alle attività d'insegnamento o al profilo professionale utilizzo delle comunicazioni elettroniche con genitori e alunni non compatibile con il ruolo professionale
2. violazione della privacy nel trattamento dei dati personali degli alunni
3. diffusione delle password
4. mancata informazione degli alunni sul corretto e responsabile uso di tecnologie e strumenti informatici e di internet
5. mancata vigilanza nell'utilizzo degli stessi
6. mancata segnalazione di situazioni critiche rispetto alla e-policy d'istituto

Le procedure di sanzione sono quelle previste dalla legge e dai contratti di lavoro

---

## ***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.

## **1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento**

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

*Il docente referente dell'e-Policy, in accordo con l'Animatore Digitale del nostro istituto e sotto la supervisione del D.S., si occuperà di rivedere ogni anno il documento di e-policy, anche attraverso interviste e sondaggi somministrati agli utenti. La revisione sarà registrata e approvata dal Collegio Docenti.*

### **Il nostro piano d'azioni**

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

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

#### **Azioni da svolgere nei prossimi 3 anni:**

- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i docenti dell'Istituto per la stesura finale dell'ePolicy.
- Organizzare incontri per la consultazione degli studenti/studentesse

sui temi dell'ePolicy per cui si evidenzia la necessità di regolamentare azioni e comportamenti.

- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i genitori dell'Istituto per la stesura finale dell'ePolicy.
- Organizzare 1 evento di presentazione 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

**Il collegio dei docenti valuta, all'inizio di ogni anno scolastico, il numero e la tipologia di azioni da implementare. Sarà possibile, inoltre, derogare al numero di azioni previsti per l'annualità laddove il collegio dei docenti ne ravvisi l'effettiva opportunità.**

# Capitolo 2 - Formazione e curriculum

---

## ***2.1. Curriculum sulle competenze digitali per gli studenti***

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

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

L'Istituto si propone di integrare il curriculum scolastico degli studenti con attività educative che favoriscano la cultura della sicurezza on line, in particolare nel primo biennio. In tal senso si impegna a sviluppare una serie di competenze e comportamenti adeguati alle età degli alunni, tra cui:

- sviluppare una serie di strategie per valutare e verificare le informazioni prima di accettare l'esattezza, sviluppando il pensiero critico;
- sapere come restringere o affinare una ricerca;
- utilizzare software per la presentazione di dati;
- sviluppare la cultura del "software libero";
- assumere comportamenti adeguati in ambienti on line, rispettosi della dignità propria e altrui;
- essere consapevoli che dati personali e fotografie possono essere manipolate e usate in maniera fraudolenta e lesiva da parte di terzi;

- comprendere che le "identità virtuali" possono essere ingannevoli;
- capire il motivo per cui non devono pubblicare foto o video di altri senza il loro permesso;
- conoscere le norme in materia di copyright;
- sviluppare una sempre maggiore sensibilità verso l'impatto che il cyberbullismo, sexting e grooming possono avere sulla vita propria e dei compagni e sapere a chi rivolgersi per segnalare abusi connessi all'utilizzo di internet;
- utilizzare con attenzione Internet per garantire che si adatti alla loro età e sia di sostegno agli obiettivi di apprendimento per le aree curriculari specifiche.

All'inizio dell'anno scolastico, i dipartimenti realizzano una o più unità di apprendimento, nell'ambito dell'insegnamento dell'Educazione Civica, finalizzate all'acquisizione di dette competenze.

---

## ***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.

In attuazione del PNSD questo Istituto ha realizzato:

- individuazione e formazione di un Animatore Digitale;
- formazione dei docenti all'utilizzo del registro elettronico e dello scrutinio elettronico;
- ampliamento della rete WI-FI/LAN dei due plessi dell'Istituto;
- ricognizione e messa a punto delle dotazioni digitali;
- attivazione della Piattaforma Didattica Google Suite for Education.

Si prevede di svolgere:

- formazione del personale in materia di sicurezza on-line;
- una politica di informazione e diffusione della e-Safety d'Istituto

- formazione sull'uso della piattaforma in uso per l'erogazione della DDI
  - formazione sulla didattica digitale integrata (DDI) (aspetti tecnici e giuridici)
  - formazione sul curriculum digitale
- 

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

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

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

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

L' Istituto s'impegna a promuovere una cultura dell'informazione, volta a coinvolgere le famiglie nella cultura di un uso consapevole delle tecnologie digitali e di internet,

attraverso:

- conoscenza e condivisione del Regolamento della Policy, al fine di garantire che i principi di omportamento sicuro on-line siano chiari;
- informazione attraverso il sito della scuola;
- incontri di consulenza con esperti;
- informazione attraverso i siti nazionali di sostegno per i genitori, quali il sito [www.generazioniconnesse.it](http://www.generazioniconnesse.it) ed altri similari.

## ***Il nostro piano d'azioni***

---

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

- Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.

### **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 e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare incontri con esperti per i docenti sulle competenze digitali e sul curriculum digitale.
- Organizzare incontri con esperti per i genitori sull'educazione alla cittadinanza digitale.

# 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.

Sono dati personali le informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, etc. L'istituzione scolastica può trattare solamente i dati personali necessari al perseguimento di specifiche finalità istituzionali, oppure quelli espressamente previsti dalla normativa di settore. Per tali trattamenti non è tenuta a chiedere il consenso degli/le studenti/esse. Alcune categorie di dati personali degli/le studenti/esse e delle famiglie, come quelli sensibili e giudiziari, devono essere trattate con estrema cautela, nel rispetto di specifiche norme di legge, verificando in primis non solo la pertinenza e completezza dei dati, ma anche la loro indispensabilità rispetto alle "finalità di rilevante interesse pubblico" che si intendono perseguire.

In casi di violazione la persona interessata (studente/essa, professore, etc.) può presentare al Garante per la Protezione dei dati personali un'apposita "segnalazione" gratuita" o un "reclamo" (più circostanziato rispetto alla semplice segnalazione e con pagamento di diritti di segreteria).

---

## **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.

L'ambiente online deve essere valutato alla stessa maniera dell'ambiente fisico, pertanto devono essere vagliati tutti gli aspetti legati alla sicurezza nel momento in cui si permette l'accesso alla rete tramite i collegamenti scolastici. Ogni aula e laboratorio del nostro Liceo, dispongono di collegamento ad Internet tramite la rete LAN della Didattica, separata dall'altra rete presente nella scuola che serve gli uffici della Presidenza e della Segreteria.

La rete Wi-Fi, che poggia sulla rete LAN della Didattica, è presente a copertura dell'intero edificio scolastico; l'accesso è consentito tramite account personale e password, fornito ai docenti per l'utilizzo nella didattica dei propri dispositivi. Tuttavia attualmente la rete wireless non è adeguata a sostenere l'accesso a tutti gli studenti della scuola. La connessione alla rete didattica è protetta da filtri che impediscono il collegamento a siti appartenenti a black list. Agli studenti è concesso l'accesso alla rete d'istituto nelle attività didattiche nei laboratori multimediali, in presenza del docente.

I computer collegati alla rete Didattica hanno 2 profili di accesso differenziato: uno riservato all'Amministratore, accessibile tramite password, e l'altro riservato agli Utenti, con accesso libero, ma limitato. È possibile effettuare installazioni e aggiornamenti di software solo tramite la password di amministratore, fornita al personale di assistenza tecnica. La rete LAN che serve la Presidenza e gli uffici della Segreteria, invece, è protetta, attraverso server, da Firewall e l'accesso ai computer è possibile solo tramite password

---

## **3.3 - Strumenti di comunicazione online**

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

I principali strumenti di comunicazione online del Liceo sono i seguenti:

### **Sito Web della scuola**

Il nostro Liceo utilizza come principale strumento di comunicazione online il sito Internet della scuola, aggiornato in tempo reale e visitato con assiduità da docenti, studenti e famiglie, a cui sono dedicate apposite sezioni. Con il nuovo Sito Internet, in fase di completamento, sarà disponibile un'Area riservata accessibile tramite Username e password. Il Dirigente Scolastico e il personale incaricato di gestire le pagine del sito della scuola hanno la responsabilità di garantire che il contenuto pubblicato sia pertinente ed appropriato all'istituzione scolastica, valutano la sicurezza e l'adeguatezza sotto il profilo dell'accessibilità e del rispetto della privacy.

Il sito della scuola è raggiungibile all'indirizzo: <http://www.iisdenobilicz.edu.it>.

### **Registro elettronico**

Il registro elettronico Axios rappresenta l'altro strumento di comunicazione online di quei dati che la scuola (Presidenza, Segreteria, docenti) vuole rendere disponibile ai destinatari (studenti e famiglia). La sicurezza e la privacy sono garantiti dal gestore mediante chiavi d'accesso individuali, generate da un'apposita procedura interna e comunicati ai destinatari attraverso comunicazione cartacea, consegnata alle famiglie, e per mezzo di posta elettronica inviata ai docenti. Attraverso la consultazione del registro elettronico online la famiglia può verificare in tempo reale alcuni dati sulla carriera scolastica del proprio figlio/a, come il curriculum scolastico; può prendere atto di assenze o ritardi e giustificazioni, può verificare i compiti assegnati dal docente, l'indicazione dell'argomento trattato, il promemoria di classe, può consultare le valutazioni. L'utilizzo del software è riservato esclusivamente ai fini didattici, nel rispetto di quanto indicato dal Software di gestione e sulla base di quanto statuito dalla normativa vigente.

### **Piattaforma didattica in cloud**

S

Il nostro Liceo ha attivato la piattaforma didattica d'Istituto GOOGLE WORKSPACE che ha prodotto la creazione di account personali di posta elettronica di tutto il personale scolastico e di tutti gli studenti e studentesse della scuola e l'attivazione di numerosi strumenti utili per la Didattica a Distanza. La registrazione degli studenti è avvenuta previa consenso informato dei genitori. La piattaforma, costruita da Google e concessa ad uso illimitato e gratuito alla scuola, è amministrata dal Dirigente Scolastico e dai suoi delegati che svolgono la funzione di Amministratori della piattaforma. E' stato stipulato un accordo tra la scuola e il proprietario dello spazio virtuale che, attraverso i suoi server, garantisce e tutela la protezione dei dati personali di tutti gli utenti, in primo luogo degli studenti. Gli Amministratori della piattaforma Google Workspace d'Istituto dispongono di strumenti agili per monitorare e gestire la sicurezza dei dati.

### **Postaelettronica**

L'accesso all'account di posta elettronica istituzionale MIUR e quello di posta certificata è riservata solo al Dirigente scolastico e al personale degli uffici di Segreteria amministrativa autorizzati. La posta elettronica è protetta da antivirus ed antispam. L'e-mail dell'istituzione scolastica, invece, attivata tramite la piattaforma G suite for education, è divenuta il tramite principale per la comunicazione tra dirigenza, segreteria, docenti ed alunni. Anch'essa è protetta da antivirus ed antispam.

---

## ***3.4 - Strumentazione personale***

I dispositivi tecnologici sono parte integrante della vita personale di ciascuno, compresa quella degli/le 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.

Nel regolamento d'Istituto non è consentito agli studenti l'utilizzo di strumenti elettronici personali ma eccezionalmente, e previa autorizzazione, può essere consentito l'uso del cellulare e/o tablet.

**Anche ai docenti è consentito, durante le lezioni, l'uso del cellulare, solo se i dispositivi scolastici siano non funzionanti. E', inoltre, consentito l'uso di altri dispositivi elettronici personali solo a scopo didattico ed integrativo di quelli scolastici disponibili.** Il presente documento dichiara indispensabile aprire all'utilizzo consapevole degli strumenti personali nella didattica da parte degli studenti ed anche consentire loro l'accesso alla rete wireless della scuola.

La scuola dovrà potenziare la rete didattica di connessione ad Internet, in modo da rendere attuabile l'uso dei dispositivi mobili a scuola, aprendo così a nuove prospettive didattiche che tali strumenti consentono.

## ***Il nostro piano d'azioni***

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

- 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
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte del personale Tecnico Amministrativo e dagli ATA

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

- Organizzare uno o più eventi o attività volti a consultare i docenti dell'Istituto per redigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali.
- Organizzare incontri per la consultazione degli studenti/studentesse sui indicazioni/regolamenti sull'uso dei dispositivi digitali personali
- Organizzare incontri per la consultazione dei genitori su indicazioni/regolamenti sull'uso dei dispositivi digitali personali
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare i genitori dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- 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)

# 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.

A tal fine l'I.I.S. "De Nobili" si propone di:

- prestare attenzione ai bisogni di tutti gli studenti,
- creare un clima scolastico positivo ed inclusivo nel rispetto delle differenze,
- sviluppare le competenze sociali degli alunni,

- prestare attenzione alle norme di gruppo nelle classi,
  - disincentivare atteggiamenti di prevaricazione,
  - effettuare indagini sul clima classe,
  - individuare la figura del referente per il bullismo,
  - intervenire tempestivamente su atteggiamenti di prevaricazione,
  - sviluppare competenze digitali e fornire informazioni riguardanti rischi e responsabilità,
  - promuovere un uso etico delle tecnologie,
  - attivare percorsi mirati in caso di individuazione di gruppi a rischio,
  - attivare, in collaborazione con famiglie ed esperti esterni, misure specifiche per casi accertati
- 

## 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).

La Scuola si impegna ad organizzare le seguenti attività di prevenzione del fenomeno:

- partecipazione da parte di docenti, studenti e genitori a convegni, seminari o corsi sul tema del bullismo e del cyberbullismo;
- interventi di consulenza e supporto su richiesta da parte della scuola relativamente a casi di cyberbullismo
- inserimento della tematica negli argomenti trattati durante le lezioni di Educazione Civica nelle classi ove se ne rilevi l'opportunità, particolarmente in quelle del biennio

**La E-Safety Policy sarà inoltre resa disponibile sul sito dell'Istituto a studenti, personale scolastico e genitori.**

---

## ***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.

- creazione di un contesto attento e sensibile nella scuola,
  - promozione progetti di impegno civico (es. service learning, raccolte, donazioni, etc.)
  - promozione di cooperative learning
  - sviluppo di social skills.
- 

## **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 Scuola promuove attività di aggregazione (es. teatro, attività motorie in squadra, etc.) e momenti di riflessione con studenti su uso consapevole delle TIC.

---

## **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 medialmente 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.

## 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.

- promozione di educazione all'affettività,
- sviluppo delle life skills),
- istituzione figura referente per segnalazioni,
- informativa sulla privacy,
- coinvolgimento polizia postale per casi accertati.

---

## 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](http://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](#).

## ***Il nostro piano d'azioni***

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

**Scegliere almeno 1 di queste azioni:**

- 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 ai genitori e ai docenti, 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/le studenti/studentesse.

# 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/le studenti/esse coinvolti/e (e quindi valutare se rivolgersi ad un servizio deputato ad offrire un supporto psicologico e/o di mediazione).
- **Adescamento online:** se si sospetta un caso di adescamento online è opportuno, innanzitutto, fare attenzione a non cancellare eventuali prove da smartphone, tablet e computer utilizzati dalla persona minorenni e inoltre è importante non sostituirsi 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 ha previsto alcuni strumenti di segnalazione ad hoc messi a loro disposizione:

- un indirizzo e-mail specifico per le segnalazioni: segnalazioni@iisdenobilicz.edu.it
- un docente referente per le segnalazioni per ognuna delle tre sedi dell'Istituto:  
sede centrale prof.ssa Mazzuca Caterina  
sede di via Pugliese Prof, Aprea Massimiliano  
sede di via Lepera Prof. Sinopoli Ivan.

Anche studenti e studentesse, inoltre, possono rivolgersi alla Helpline del progetto

Generazioni Connesse, al numero gratuito [1.96.96](tel:1.96.96).

Per le segnalazioni di fatti rilevati sono previsti i seguenti strumenti che i docenti possono utilizzare sulla base della gravità dell'accaduto:

- annotazione del comportamento sul registro e comunicazione scritta ai genitori, che la devono restituire vistata;
- convocazione scritta e colloquio con i genitori degli alunni, da parte dei docenti;
- relazione scritta al Dirigente scolastico.

Per i reati più gravi (es. pedopornografia) gli operatori scolastici hanno l'obbligo di effettuare la denuncia all'autorità giudiziaria (o più semplicemente agli organi di polizia territorialmente competenti). In particolare per i fatti criminosi, ai fini della denuncia, la relazione deve essere redatta nel modo più accurato possibile, indicando i seguenti elementi: il fatto, il giorno dell'acquisizione del fatto nonché le fonti di prova già note e per quanto possibile, le generalità, il domicilio e quant'altro di utile a identificare la persona alla quale il reato è attribuito, la persona offesa, e tutti coloro che sono in grado di riferire circostanze rilevanti per la ricostruzione del fatto.

**Email per le segnalazioni: [segnalazioni@istitutodebobili.gov.it](mailto:segnalazioni@istitutodebobili.gov.it)**

---

### **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.

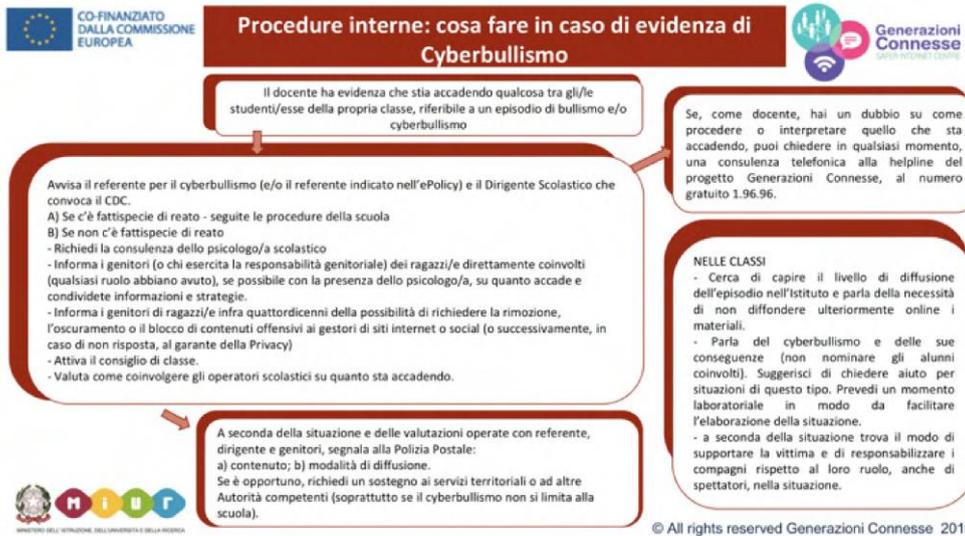
Per una mappatura degli indirizzi di tali strutture è possibile consultare il [Vademecum](#) di Generazioni Connesse "Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all'utilizzo delle tecnologie digitali da parte dei più giovani" (seconda parte, pag. 31), senza 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.

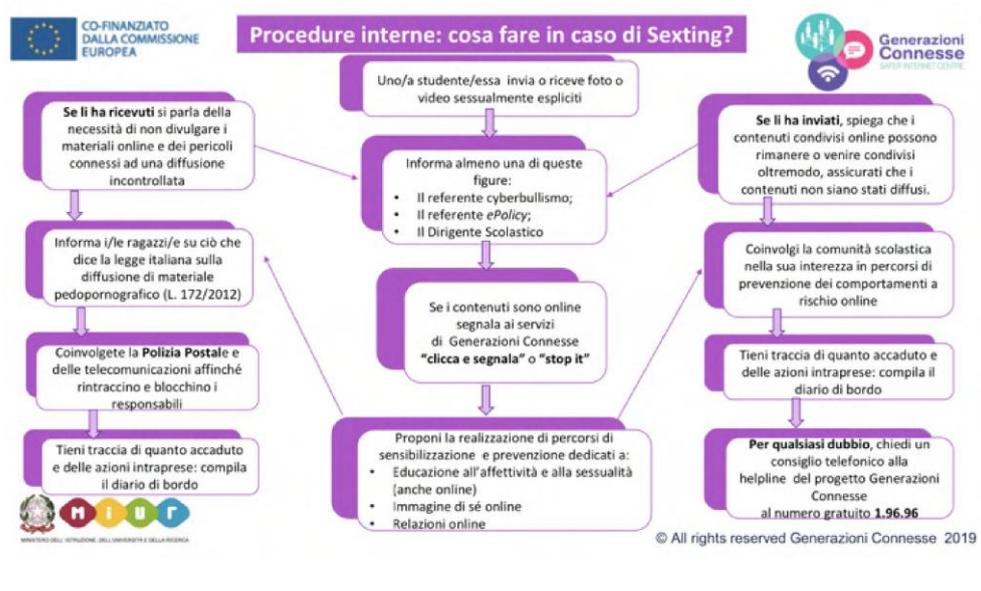
- **Comitato Regionale Unicef:** laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni):** svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare 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***

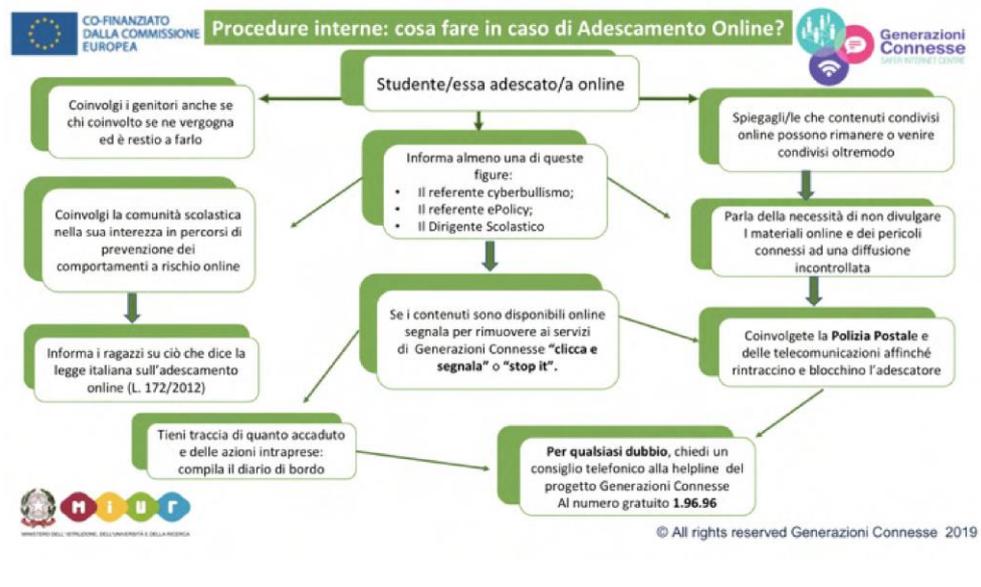
### **Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?**



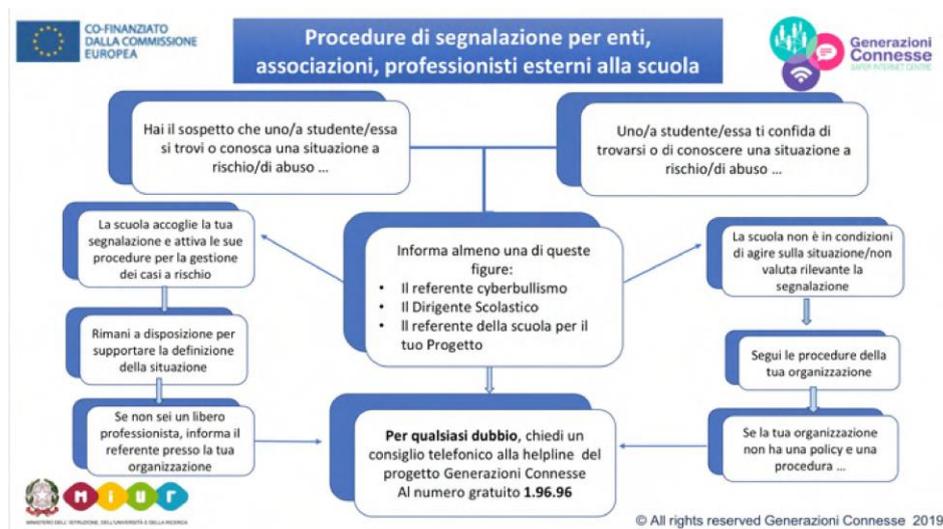
## Procedure interne: cosa fare in caso di sexting?



## 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***

Dal momento dell'approvazione del presente documento di ePolicy, la Scuola si impegna a diffonderlo portandolo a conoscenza di tutti i soggetti interessati tramite sito web o incontri mirati.

La scuola si impegna, inoltre, ad inserire nel curriculum della disciplina Educazione Civica tematiche relative a bullismo, cyberbullismo e rischi on line.

- applicare le procedure indicate, utilizzare gli strumenti della scheda di segnalazione, del diario di bordo, della cassetta di segnalazione e della mail finalizzata allo scopo.

