



Documento di ePolicy

Rev3 del 29/10/2025

IC Giampaolo Gamera- PIIC81800R -Via Ximenes 1 56121 Pisa

Indice

Capitolo 1 - Introduzione al documento di ePolicy	3
1.1. Scopo dell'ePolicy	3
1.2. Perché è importante dotarsi di una ePolicy?	3
1.3. Ruoli e responsabilità	3
1.4. Un'informativa per i soggetti esterni che erogano attività educative dell'Istituto	5
1.5. Condivisione e comunicazione dell'e-Policy all'intera comunità scolastica	6
1.6. Gestione delle infrazioni alla ePolicy	7
1.7. Integrazione dell'ePolicy con i Regolamenti	7
1.8. Monitoraggio dell'implementazione della ePolicy e suo aggiornamento	7
1.9. Piano d'azioni per la diffusione dell'ePolicy	7
1.10. Piano d'azioni per la diffusione dell' ePolicy	8
Capitolo 2	9
Sensibilizzazione e prevenzione	9
Questo capitolo raccoglie indicazioni su azioni formative per studenti/esse, famiglie e docenti con obiettivi a breve e lungo termine e riferimenti normativi (es legge 92 2019 su ECD). I rischi online andranno in appendice come glossario, sul sito come approfondimenti, sul kit didattico come attività.	9
2.1. Sensibilizzazione e prevenzione	9
2.2. Curricolo sulle competenze digitali per gli alunni	9
2.3. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC	10
2.4. Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali	10
2.5. Sensibilizzazione delle famiglie e integrazioni al Patto di Corresponsabilità	10
2.6. Formazione sull'uso consapevole delle T.I.C.	10
Capitolo 3	12
Gestione dell'infrastruttura e dell'strumentazione TIC della e nella scuola	12
3.1. Protezione dei dati personali e GDPR	12
3.2. Strumenti di comunicazione online (PUA)	13
3.4. Piano d'azione sugli strumenti TIC	13
3.4.1. AZIONI da sviluppare nell'A.S. 2024-25	13
3.5.2. AZIONI da sviluppare nel triennio 2025-28	13
Capitolo 4 - Rischi on line: conoscere, prevenire e rilevare	15
4.1. Sensibilizzazione e Prevenzione	15
4.2. Cyberbullismo: che cos'è e come prevenirlo	15
4.3. Hate speech: che cos'è e come prevenirlo	16
4.7. Pedopornografia	18
4.8. Piano d'azione	18
Capitolo 5 - Segnalazione e gestione dei casi	20
5.1. Cosa segnalare	20
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?	24
Procedure interne: cosa fare in caso di sexting?	25
Procedure interne: cosa fare in caso di adescamento online?	25
Procedure di segnalazione per enti, associazioni, professionisti esterni alla scuola	26
Il nostro piano d'azioni	26

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 alunni e delle alunne.

Quella digitale è una competenza chiave del cittadino europeo, come indicato dal Consiglio Europeo (Raccomandazione del 2018) che permette a ogni cittadino di esercitare i propri diritti all'interno degli ambienti digitali (ONU - [Commento Generale 25](#): I diritti dei minori negli ambienti digitali).

In un contesto sempre più complesso, diventa, quindi, essenziale per ogni Istituto Scolastico dotarsi di una ePolicy, un documento programmatico volto a promuovere le competenze digitali e un uso delle tecnologie positivo, critico e consapevole, sia da parte dei ragazzi e delle ragazze, che degli adulti coinvolti nel processo educativo. L'ePolicy, inoltre, è un documento finalizzato a prevenire situazioni problematiche e a riconoscere, gestire, segnalare e monitorare episodi legati ad un utilizzo scorretto degli strumenti.

L'ePolicy 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 (TIC) 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.

1.2. Perché è importante dotarsi di una ePolicy?

Attraverso l'ePolicy 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' ePolicy 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 ed educative con le tecnologie digitali, oltre che di sensibilizzazione su un uso consapevole delle stesse.

1.3. Ruoli e responsabilità

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, si impegni nella sua attuazione e promozione.

Il Dirigente scolastico

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

- promuovere la cultura della sicurezza online e garantirla a tutti i membri della comunità scolastica, in linea con il quadro normativo di riferimento, le indicazioni del MIM, delle sue agenzie e attraverso il documento di ePolicy;
- promuovere la cultura della sicurezza online, anche attraverso il documento di ePolicy, integrandola e inserendola nelle misure di sicurezza più generali dell'intero Istituto;
- fornire sistemi per un uso sicuro delle TIC, internet, i suoi strumenti e ambienti e deve garantire alla popolazione scolastica la sicurezza di navigazione tramite internet, utilizzando adeguati sistemi informatici e filtri;
- ha la responsabilità della gestione dei dati e della sicurezza delle informazioni e garantisce che l'Istituto segua le pratiche migliori possibili nella gestione dei dati stessi;
- tutelare la scuola e garantire agli utenti la sicurezza di navigazione utilizzando adeguati sistemi informatici e servizi di filtri Internet;
- ha il compito di garantire a tutto il personale una formazione adeguata sulla sicurezza online per essere tutelato nell'esercizio del proprio ruolo educativo e non;
- essere a conoscenza delle procedure da seguire in caso di un grave incidente di sicurezza online;
- garantire adeguate valutazioni di rischio nell'usare strumenti e TIC, effettuate in modo che quanto programmato possa soddisfare le istanze educative e didattiche dichiarate nel PTOF di Istituto;
- garantire l'esistenza di un sistema che assicuri il monitoraggio e il controllo interno della sicurezza online in collaborazione con le figure di sistema.

Il Referente d'Istituto per la prevenzione ed il contrasto del Bullismo e del Cyberbullismo, individuato ai sensi dell'art. 4, comma 3, Legge 29 maggio 2017, n. 71, ha il compito di "coordinare le iniziative di prevenzione e di contrasto del cyberbullismo, anche avvalendosi della collaborazione delle Forze di polizia, nonché delle associazioni e dei centri di aggregazione giovanile presenti sul territorio". Il suo ruolo è fondamentale non solo in ambito scolastico, ma anche in quello extrascolastico, ove possibile, per il coinvolgimento di percorsi formativi finalizzati per alunni e alunne, per genitori e per l'intera comunità scolastica.

IL TEAM ANTIBULLISMO E PER L'EMERGENZA. In coerenza con le Linee di Orientamento per la prevenzione e il contrasto del Bullismo e Cyberbullismo del Ministero dell'Istruzione (D.M. n. 18 del 13/1/2021, agg. 2021 – nota prot. 482 del 18-02-2021), il Team, costituito dai Referenti sul bullismo e cyberbullismo di ogni plesso, ha le funzioni di coadiuvare il Dirigente Scolastico nella definizione degli interventi di prevenzione e nella gestione dei casi di bullismo e cyberbullismo che si possono presentare. Promuove, inoltre, la conoscenza e la consapevolezza del bullismo e del cyberbullismo attraverso progetti d'istituto che coinvolgano genitori, studenti e tutto il personale e comunica ad alunni, famiglie e tutto il personale scolastico dell'esistenza del team, a cui poter fare riferimento per segnalazioni o richieste di informazioni sul tema.

L'Animatore digitale rappresenta un valido supporto per l'intero personale scolastico, non solo dal punto di vista tecnico-informatico, ma anche in riferimento alla protezione e gestione dei dati personali, rischi online, e per buone prassi in materia di percorsi di formazione "scuola digitale" ed "educazione civica".

I/le docenti hanno un ruolo centrale nel diffondere la cultura dell'uso responsabile delle TIC e della Rete. Possono, innanzitutto, integrare la propria disciplina con approfondimenti, promuovendo l'uso delle tecnologie digitali nella didattica. I docenti devono accompagnare e supportare gli/le studenti nelle attività di apprendimento e nei laboratori che prevedono l'uso della Digital Board o di altri dispositivi tecnologici che si connettono alla Rete. Inoltre, educano gli studenti alla prudenza, a non fornire dati ed informazioni personali, ad abbandonare un sito dai contenuti che possono turbare o spaventare e a non incontrare persone conosciute in Rete. Informano gli alunni sui rischi presenti in Rete, senza demonizzarla, ma sollecitandone un uso consapevole, in modo che Internet possa rimanere per bambini/e e ragazzi/e una fonte di divertimento e uno strumento di apprendimento. I/le docenti osservano regolarmente i comportamenti a rischio sia dei potenziali bulli, sia delle potenziali vittime e hanno il dovere morale e professionale di segnalare qualunque problematica, violazione o abuso, anche online, che veda coinvolti studenti e studentesse, dandone tempestiva comunicazione al Dirigente Scolastico, al Referente per il Cyberbullismo e Bullismo e al Consiglio di Classe per definire strategie di intervento condivise.

Il Responsabile della protezione dei dati (DPO) conosce l'ePolicy di Istituto, fornisce la propria consulenza in merito agli obblighi derivanti dal GDPR e sorveglia sull'esatta osservanza della normativa in materia di tutela dei dati personali ed è co-responsabile delle azioni di informazione e formazione nell'Istituto sulla protezione dei dati personali.

Il Personale Amministrativo, Tecnico ed Ausiliario (ATA), svolge funzioni di tipo amministrativo, contabile, gestionale e di sorveglianza, connesse alle attività dell'Istituzione scolastica, in collaborazione con il Dirigente scolastico e con il personale docente tutto. È coinvolto nella segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo insieme alle figure interne preposte. Raccoglie, verifica e valuta le informazioni inerenti a possibili casi di bullismo e di cyberbullismo.

Gli alunni e le alunne sono tenuti/e al rispetto delle norme che disciplinano l'utilizzo consapevole delle tecnologie digitali con la finalità di salvaguardare la propria identità e quella altrui, secondo quanto indicato nel Regolamento d'Istituto. La partecipazione a percorsi formativi e progettuali ha lo scopo di promuovere l'utilizzo positivo delle TIC e della Rete, in una dimensione di *peer education*. I genitori sono corresponsabili nelle scelte educative dell'Istituzione scolastica, atte alle attività di prevenzione ed uso consapevole delle TIC, della Rete e dei device personali dei rispettivi figli.

I Genitori/Adulti di riferimento, in continuità con l'Istituto scolastico, sono attori partecipi e attivi nelle azioni di promozione ed educazione sull'uso consapevole delle TIC e della Rete, nonché sull'uso responsabile degli strumenti personali (pc, smartphone, etc). Come parte della comunità educante, sono tenuti a relazionarsi in modo costruttivo con i/le docenti sulle linee educative che riguardano le TIC e la Rete e, ivi incluso il documento di ePolicy, comunicare con loro circa i problemi rilevati quando i/le propri/e figli/e non usano responsabilmente le tecnologie digitali o Internet. È estremamente importante che accettino e condividano quanto scritto nell'ePolicy d'Istituto e nel Patto di Corresponsabilità in un'ottica di collaborazione reciproca. Si promuove il coinvolgimento dei rappresentanti di genitori/adulti di riferimento all'interno del percorso di definizione e implementazione dell'ePolicy.

Gli Enti educativi esterni e le Associazioni che entrano in relazione con l'Istituzione scolastica, osservano le politiche interne sull'uso consapevole della Rete e delle TIC, fermo restando l'obbligo di attivare procedure e comportamenti sicuri per la protezione degli alunni e delle alunne, durante le attività che vengono svolte all'interno della scuola o in cui sono impegnati gli stessi.

Per quanto non espressamente indicato sui ruoli e sulle responsabilità delle figure presenti all'interno dell'Istituzione scolastica, si rimanda: all'art. 21, comma 8, Legge 15 marzo 1997, n. 59; all'art. 25 della Legge 30 marzo 2001, n. 165; al CCNL in vigore; al D.P.R. 8 marzo 1999, n. 275; alla Legge 13 luglio 2015, n. 107; al Piano Nazionale Scuola Digitale; a quanto statuito in materia di culpa in vigilando, culpa in organizzando, culpa in educando.

1.4. Un'informativa per i soggetti esterni che erogano attività educative dell'Istituto

Tutti gli attori che entrano in relazione educativa con gli alunni e le alunne devono:

- mantenere sempre un elevato profilo personale e professionale, eliminando atteggiamenti inappropriati;
- essere guidati dal principio dell'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 alunni e delle alunne, oltre che quelli legati a tollerare o partecipare a comportamenti di minori che

siano 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 nelle quali 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 alunni e le alunne. 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).

1.5. Condivisione e comunicazione dell'e-Policy all'intera comunità scolastica

Il documento di ePolicy viene condiviso con tutta la comunità educante, ponendo al centro gli alunni e le alunne e sottolineando compiti, funzioni e attività reciproche. È molto importante che ciascun attore scolastico (dai docenti agli/alle alunni/e) si faccia a sua volta promotore del documento.

1. Informazione della comunità educante (in particolare le famiglie) sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali con relative informative.

L'efficacia dell'ePolicy è direttamente proporzionale a livello di conoscenza e diffusione all'interno della comunità scolastica ivi comprese le famiglie. Il documento rappresenta il canale interno privilegiato per informare, responsabilizzare e collaborare sui temi della rete e delle tecnologie a scuola con l'intera comunità scolastica. In tal senso, il documento è accompagnato da versioni, allegate e sintetiche, all'interno delle quali sono individuati gli elementi principali del documento; una versione è diretta agli studenti ed una è diretta alle famiglie con un linguaggio e una presentazione dei contenuti adeguata, flessibile e chiara. La versione sintetica rivolta agli studenti è inserita all'interno delle attività didattiche dell'educazione alla cittadinanza mentre la versione per le famiglie è consegnata nel corso dei colloqui scuola-famiglia. Il documento è altresì pubblicato sul sito della scuola ed inserito nel Patto di corresponsabilità.

2. Come comunicare e condividere l'ePolicy con gli attori pubblici e privati (enti, aziende, associazioni, etc) che realizzano iniziative nelle scuole sui temi dell'educazione civica digitale con relative informative).

La presenza dell'ePolicy nell'Istituto scolastico è garanzia, per il territorio, della presenza di un presidio informato, sensibile e attento sulla rete e le tecnologie in relazione con i più giovani. In questo senso l'Istituto può rappresentare per le Istituzioni del territorio, le aziende, e le realtà del Terzo Settore un luogo di confronto privilegiato e di sperimentazione per tutti coloro che intendono costruire progetti di cittadinanza digitale rivolte ai più giovani. A tal fine l'adozione dell'ePolicy è comunicata all'USR di riferimento e al Municipio (servizi istruzione e servizi sociali) attraverso gli allegati sintetici progettati che indicano gli elementi del documento e le prospettive per la comunità.

1.6. Gestione delle infrazioni alla ePolicy

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

Il gruppo di lavoro ePolicy proporrà alla comunità scolastica nell'anno scolastico 2024-25 alcuni regolamenti con eventuali sanzioni disciplinari da allegare al presente Documento.

Tali regolamenti individuano le mancanze disciplinari, le azioni educative e/o sanzioni relative e i soggetti eroganti in modo predefinito e certo.

1.7. Integrazione dell'ePolicy con i Regolamenti

La trasversalità dell'ePolicy rende necessaria una sua integrazione nell'ambito dei documenti che disciplinano il funzionamento dell'Istituto Scolastico. Il Regolamento dell'Istituto scolastico, che rappresenta il principale punto di riferimento normativo, dovrà essere aggiornato in modo tale da dare contezza dell'adozione dell'ePolicy, e richiamare

le norme comportamentali e le procedure di utilizzo delle Tecnologie dell'Informazione e della Comunicazione in ambiente scolastico.

Anche il **Patto di Corresponsabilità educativa** tra scuola e famiglia dovrà essere integrato con gli opportuni riferimenti all'ePolicy, puntualizzando, da un lato l'impegno dell'Istituto ad organizzare eventi formativi/informativi a beneficio dei genitori, e dall'altro l'impegno di questi ultimi a partecipare in maniera proattiva a tali eventi.

Il Piano Triennale dell'Offerta Formativa, per la sua funzione di carta d'identità culturale e progettuale delle istituzioni scolastiche, nel quale si esplicita la progettazione curricolare, extracurricolare, educativa e organizzativa che le singole scuole adottano nell'ambito della loro autonomia, deve contenere anche le progettualità relative ad azioni media educative legate al percorso di ePolicy. Così come il PTOF è il risultato di una consapevole concertazione fra le componenti delle istituzioni scolastiche (Dirigente Scolastico, docenti, alunni, genitori) e fra queste e il territorio, il patto di corresponsabilità rappresenta l'assunzione di responsabilità da parte di tutti coloro che svolgono un ruolo attivo nella Comunità educante.

1.8. Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

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

Il monitoraggio e la revisione del documento ePolicy viene affidato al docente Referente ePolicy coadiuvato dal gruppo di lavoro e, ove possibile, con la partecipazione dell'animatore digitale.

1.9. Piano d'azioni per la diffusione dell'ePolicy

I piani di azione rappresentano il programma triennale di obiettivi che la scuola intende realizzare per promuovere la conoscenza delle regole e dei protocolli di intervento, i quali sono stati adottati con il documento di ePolicy nella comunità scolastica.

Nei Piani di Azione sono riportati gli impegni e le responsabilità che la scuola si assume per promuovere i temi dell'educazione civica digitale e dell'utilizzo sicuro e consapevole delle tecnologie e della rete. Inoltre, si impegna a effettuare la rilevazione dei bisogni, a promuovere iniziative informative e formative, la formazione di docenti, studenti e studentesse. La scuola si interessa del monitoraggio e della valutazione delle azioni, ove possibile, anche all'interno del RAV.

I Piani di Azione si distinguono tra standard, comuni a ogni scuola che ha adottato l'ePolicy e autoprodotti, ovvero definiti dalla scuola sulla base del proprio contesto territoriale e delle collaborazioni in essere con Istituzioni, associazioni e aziende.

1° ANNO DI ATTIVITA' CON L' ePOLICY

MODULO I

Realizzare un evento di presentazione dell' ePolicy ai docenti dell'Istituto; realizzare un evento di diffusione dell'ePolicy in occasione degli Open Day e/o in occasione del SID (Safe Internet Day) dell'Istituto dedicato alle famiglie ed a studenti/esse.

MODULO II

Effettuare una rilevazione del fabbisogno formativo dei docenti sui temi dell'educazione civica digitale; effettuare una rilevazione di interessi, bisogni e comportamenti delle famiglie sull' uso positivo del digitale; avviare l'introduzione del kit didattico come metodo e risorsa di lavoro in alcune classi pilota.

2° ANNO DI ATTIVITA' CON L'ePOLICY**MODULO I**

Diffondere l' ePolicy negli ambienti scolastici, a studenti e studentesse, docenti e famiglie attraverso le versioni friendly dell'ePolicy.

MODULO II

Integrare l' ePolicy (norme, regolamenti e procedure) nei documenti dell'Istituto; aggiornare la Politica d'Uso Accettabile (PUA) della scuola.

MODULO III

Definizione, a partire da quanto definito nell'ePolicy, delle procedure di segnalazione anche con linguaggio child/youth friendly perché possano essere accessibili a studenti e studentesse; realizzare una reportistica delle segnalazioni ricevute e dei relativi esiti.

3° ANNO DI ATTIVITA' CON L' EPOLICY**MODULO I**

Realizzare una formazione rivolta ai docenti dell'Istituto, sulla base dei risultati della rilevazione svolta nel corso del primo anno, anche attraverso il supporto di esperti/associazioni esterne o avvalendosi del percorso disponibile sul sito di Generazioni Connesse. La formazione deve coprire almeno il 60% del corpo docente.

MODULO II

L'istituto utilizza il kit didattico come pratica metodologica e risorse a disposizione dei docenti per i percorsi di ECD attraverso la formazione specifica sviluppata per i docenti attraverso il sito di Generazioni Connesse; effettuare una rilevazione di interessi, bisogni, comportamenti, abitudini di studenti e studentesse sui temi dell'educazione civica digitale; realizzare una formazione rivolta agli studenti e alle studentesse attraverso il percorso previsto sulla piattaforma di Generazioni Connesse; realizzare una formazione rivolta alle famiglie attraverso il percorso previsto sulla piattaforma di Generazioni Connesse.

1.10. Piano d'azioni per la diffusione dell' ePolicy

Risorse di Generazioni Connesse:

[Kit Didattico](#) Area formazione (per docenti, famiglie, studenti/sse con ePolicy)

[Canale Youtube](#) (webinar, video-stimolo, serie per target differenti)

Canale [TikTok](#)

Canale [Instagram](#)

Canale [Facebook](#)

Capitolo 2

Sensibilizzazione e prevenzione

Questo capitolo raccoglie indicazioni su azioni formative per studenti/esse, famiglie e docenti con obiettivi a breve e lungo termine e riferimenti normativi (es legge 92 2019 su ECD). I rischi online andranno in appendice come glossario, sul sito come approfondimenti, sul kit didattico come attività.

2.1. Sensibilizzazione e prevenzione

La quotidianità in rete di ciascuno dei componenti della comunità scolastica - docenti, studenti e famiglie - deve essere caratterizzata da una consapevolezza critica delle caratteristiche degli ambienti e dei servizi online affiancata alle competenze per vivere al meglio il mondo connesso. In questa direzione l'ePolicy è un documento che sviluppa azioni e interventi con l'obiettivo di raggiungere l'intera comunità scolastica e promuovere, ciascuno secondo il proprio ruolo, una cittadinanza digitale composta dalla conoscenza dei diritti in rete, dei rischi e delle opportunità per una partecipazione attiva e responsabile nella rete.

2.2. Curricolo sulle competenze digitali per gli alunni

Gli alunni utilizzano 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 alunni e le alunne verso un uso consapevole e responsabile delle tecnologie digitali. Ciò avverrà attraverso la progettazione e implementazione di un curricolo digitale.

La formazione del curricolo digitale non può non tener conto di quanto disposto dall'art. 5 della legge 20 agosto 2019 n. 92 (Introduzione dell'insegnamento scolastico dell'educazione civica) interamente dedicato alla "cittadinanza digitale" intesa come capacità di un individuo di avvalersi consapevolmente e responsabilmente dei mezzi di comunicazione virtuali.

Sono state individuate le seguenti aree tematiche:

- 1° anno: Riconoscere i rischi del *web* e saper informarsi contro le Fake news.
- 2° anno: Dipendenze e rete internet.
- 3° anno: Difesa e protezione dei dati.

Ogni nucleo tematico sarà sviluppato in termini di contenuti, abilità e competenze e acquisizione di specifici atteggiamenti in capo ai discenti.

2.3. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC

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 alunni e alle alunne modelli di utilizzo positivo, critico e specifico delle nuove tecnologie e per armonizzare gli apprendimenti.

In linea con i percorsi individuati nel PTOF 2022-25, il nostro istituto organizza costantemente corsi di formazione per l'utilizzo delle TIC, a beneficio di tutto il corpo docente ricorrendo a figure esperte sia interne che esterne.

2.4. 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 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, EFT, Osservatori regionali sul bullismo, scuole Polo, etc...), delle amministrazioni comunali, dei servizi socio-educativi e delle associazioni presenti.

2.5. 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.

2.6. Formazione sull'uso consapevole delle T.I.C.

2.6.1. AZIONI da sviluppare nell' A.S. 2025-26

- Effettuare un'analisi del fabbisogno formativo su un campione di alunni e alunne 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.
- 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.

2.6.2. AZIONI da sviluppare nel triennio 2025-2028

- 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 consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare incontri con esperti sulle competenze digitali per i docenti.
- Organizzare incontri per i genitori con esperti sull'educazione alla cittadinanza digitale.

Capitolo 3

Gestione dell'infrastruttura e della strumentazione TIC della e nella scuola

3.1. Protezione dei dati personali e GDPR

“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 alunni 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.

Il nostro Istituto si è prontamente adeguato alla suindicata normativa adempiendo a quanto in essa prescritto. È stata attivata una specifica sezione Privacy sul sito web dell'istituto dove sono state pubblicate tutte le informative e i relativi moduli per l'acquisizione dei consensi, i dati del DPO, la politica sulla protezione dei dati personali, il vademecum “La scuola a prova di Privacy”, organigramma e funzionigramma Privacy, infine si è provveduto a dotarsi del registro dei trattamenti nonché degli accorgimenti tecnici e strutturali idonei al fine di tutelare il diritto alla riservatezza dei componenti la comunità scolastica.

3.2. Strumenti di comunicazione online (PUA)

La Politica d'Uso Accettabile e Responsabile della Rete (P.U.A.) è un documento che racchiude una serie di regole legate all'utilizzo della rete a scuola e a casa da parte di studenti e di tutto il personale (compresi i professionisti esterni che lavorano in contesto scolastico), integrante il DPS (Documento programmatico sulla Sicurezza). Il documento, che funge da raccordo, si compone di punti strategici riguardanti non solo i vantaggi di internet a scuola ma anche i rischi connessi all'online, nella valutazione di quei contenuti presenti in rete e di quelle azioni negative che possono comprometterne l'uso positivo. Fra queste attività: ricercare materiale non consono allo stile educativo della scuola; produrre vere e proprie azioni illecite; giocare online con la rete scolastica; violare la privacy e i diritti d'autore, etc... Nella Politica d'Uso Accettabile e Responsabile della Rete (P.U.A.) vengono definite, dunque, le regole di utilizzo fra tutti gli attori in gioco, nel rispetto dei dati sensibili di ciascuno, in particolar modo degli alunni e delle alunne.

3.3. *Strumentazione personale (BYOD)*

I dispositivi tecnologici sono parte integrante della vita personale di ciascuno, compresa quella degli/delle alunni/e 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 MIM 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.

Il nostro istituto si è dotato di una regolamentazione condivisa e specifica su tali aspetti per la quale si rinvia al Regolamento d'Istituto 2023-24.

3.4. Piano d'azione sugli strumenti TIC

3.4.1. AZIONI da sviluppare nell'A.S. 2025-26

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli alunni e delle alunne.
- 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 .

3.5.2. AZIONI da sviluppare nel triennio 2025-28

- 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 alunni/alunne su 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 alunni e le alunne 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 alunni e le alunne 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 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**.

Per ciò che concerne la **sensibilizzazione**, le azioni da adottare devono avere l'obiettivo 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.

La **prevenzione** è un insieme di attività, azioni e 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 alunni (ed ex alunni) 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.

- previsione di 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 Referente per la prevenzione e il contrasto al Cyberbullismo, avrà il compito di:

- creare una consapevolezza diffusa sulla presenza del bullismo all'interno delle Istituzioni Scolastiche e formative di ogni ordine e grado;
- accrescere le capacità di intervento, sia in ottica preventiva, sia di gestione degli episodi già verificatisi;
- approfondire la conoscenza delle tecnologie digitali, del funzionamento del web, delle dinamiche dei social network;
- coinvolgere diversi attori, con particolare attenzione ai genitori e alle realtà aggregative territoriali, per garantire la promozione di azioni di prevenzione e contrasto anche in contesti diversi da quello strettamente scolastico;
- diffondere e replicare le iniziative su tutto il territorio di riferimento, valorizzando le buone prassi già sperimentate;
- interiorizzare e potenziare le competenze sociali e civiche;
- promuovere negli alunni comportamenti empatici e pro sociali;
- promuovere negli alunni buone prassi comportamentali;
- promuovere la sicurezza in Rete degli alunni, perché acquisiscano le competenze necessarie all'esercizio di una cittadinanza digitale consapevole;
- realizzare un'alfabetizzazione emotiva, individuando nell'analfabetismo emotivo, accresciuto dai mezzi tecnologici, la causa prima di atteggiamenti sociali violenti e intenzionali, di natura sia fisica che psicologica;
- promuovere la costruzione di un ambiente emotivamente sano, perché esso costituisce un terreno fertile per l'apprendimento e la socializzazione, sposando a pieno il concetto di "intelligenza emotiva" (Goleman, 1990) che vuole occuparsi prima delle emozioni dei ragazzi e poi delle loro abilità e talenti;
- supportare docenti e famiglie in momenti di difficoltà;
- divulgare l'importanza e la necessità del rapporto con l'adulto come guida autorevole.

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 è estremamente importante affrontarlo anche a livello educativo e scolastico con l'obiettivo di:

- fornire agli alunni 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.

Sono in fase di progettazione le azioni che il nostro Istituto intende intraprendere per il prossimo anno scolastico in relazione a questa problematica.

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.

La nostra scuola presta particolare attenzione ai segnali comportamentali degli alunni e delle alunne da cui si può evincere un attaccamento morboso al gioco online o all'abuso di navigazione virtuale, informando preventivamente i genitori e proponendo percorsi rieducativi con i docenti di informatica o, nei casi di dipendenza più gravi, il rinvio allo Sportello d'ascolto per l'adozione di un intervento personalizzato.

L'istituto promuoverà azioni di prevenzione attraverso percorsi sul benessere digitale.

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 medialti 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 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.

Sono in fase di progettazione per il prossimo anno scolastico le azioni che il nostro Istituto intende intraprendere per prevenire ed affrontare la delicata problematica dell'adescamento.

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](#).

Su tale problematica verrà realizzata dal nostro istituto nel prossimo anno scolastico, un’attività di sensibilizzazione rivolta ai genitori e al personale scolastico promuovendo i servizi di Generazioni Connesse.

4.8. Piano d'azione

4.8.1. AZIONI da sviluppare nell’A.S. 2025-26

- Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti a alunne e alunni.
- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all’utilizzo delle tecnologie digitali, rivolti a alunne e alunni, con il coinvolgimento di esperti.
- 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.
- Organizzare uno o più incontri di formazione all’utilizzo sicuro e consapevole di Internet e delle tecnologie digitali integrando lo svolgimento della didattica e assicurando la partecipazione attiva degli alunni/alunne.

4.8.2. AZIONI da sviluppare nel triennio 2025-28

- Promuovere incontri e laboratori per alunni e alunne 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 di alunne e alunni.

- Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti a alunne e alunni.
- Organizzare uno o più eventi e/o dibattiti in momenti extra-scolastici, sui temi della diversità e sull'inclusione rivolti a genitori, alunni/alunne 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 alunni e alunne (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 alunni/e 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 alunni e alunne, 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 alunni e le alunne e il personale della scuola, con l'utilizzo di locandine da affiggere a scuola, attraverso news nel sito della scuola, durante i collegi dei 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/alte alunni/e 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 (ex art. 357 c.p.) 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.

Il Codice Penale Italiano, all'art. 357, definisce il pubblico ufficiale come colui che esercita una "pubblica funzione legislativa, giudiziaria o amministrativa". Questa definizione si estende ai docenti nel momento in cui sono impegnati nell'esercizio delle loro funzioni all'interno degli istituti scolastici.

La Corte di Cassazione, con la sentenza n. 15367/2014, ha ribadito la qualifica di pubblico ufficiale per l'insegnante, estendendo tale riconoscimento non solo alla tenuta delle lezioni, ma anche a tutte le attività connesse. Questo include, ad esempio, gli incontri con i genitori degli allievi.

Le situazioni problematiche in relazione all'uso delle tecnologie digitali dovrebbero essere sempre gestite da un team di docenti composto da:

1. Dirigente
2. Docente referente,
3. L'animatore digitale (secondo il Piano Nazionale per la Scuola Digitale, abbreviato in PNSD, introdotto dalla Legge 107/2015)
4. Referente bullismo (ex. Legge Italiana Contro il Cyberbullismo, l. 71/2017)
5. Altri docenti già impegnati nelle attività di promozione dell'educazione civica.

Le situazioni di pregiudizio presunto o reale possono richiedere il supporto e l'intervento di esperti esterni alla scuola.

Strumenti a disposizione di alunni/e

Per aiutare alunni/e 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:

- 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 alunni e alunne, inoltre, possono rivolgersi alla Helpline del progetto Generazioni Connesse, al numero gratuito **1.96.96**.

Per ulteriori chiarimenti in merito, si rimanda al Regolamento di disciplina degli studenti e delle studentesse, integrato con la previsione di infrazioni disciplinari legate a comportamenti scorretti assunti durante la DID e relative sanzioni, alle [Linee di Orientamento per la prevenzione e il contrasto dei fenomeni di Bullismo e Cyberbullismo del MI \(Ministero dell'Istruzione\)](#) aggiornate al 2021, al Patto educativo di corresponsabilità e annessa appendice relativa agli impegni che le parti in causa dovranno assumere per l'espletamento efficace della DID e, in ultimo, al Piano scolastico per la Didattica Digitale Integrata, allegato al PTOF.

Come descritto nelle procedure di questa sezione, si potrebbero palesare due macro - 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. In questo caso, l'informazione relativa al sospetto deve essere inoltrata al Referente e al team dei docenti "antibullismo" con l'obiettivo di allertare il Dirigente. La comunicazione dovrebbe avere una forma scritta e riportare tutti i dati e le informazioni in maniera dettagliata e oggettiva. Da qui, il Dirigente e i docenti coinvolti procedono alla valutazione del caso (valutare l'invio o meno della relazione agli organi giudiziari preposti) e agiscono tramite percorsi di sensibilizzazione.

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.

In questo caso, l'informazione relativa al sospetto deve essere inoltrata al Referente e al team dei docenti "antibullismo" con l'obiettivo di allertare il Dirigente. La comunicazione dovrebbe avere una forma scritta e riportare tutti i dati e le informazioni in maniera dettagliata e oggettiva. Da qui, si procede alla valutazione approfondita e alla verifica di quanto segnalato, avviando (se appurato la rilevanza penale) la procedura giudiziaria con denuncia all'autorità giudiziaria per attivare un procedimento penale. Qualora si rilevasse un fatto riconducibile alla fattispecie di reato, l'insegnante - nel ruolo di pubblico ufficiale – non deve procedere con indagini di accertamento ma ha sempre l'obbligo di segnalare l'evento all'autorità giudiziaria. (ex. l. 71/2017). Con autorità competente si intendono: Procure Ordinarie: nel caso in cui il minore/i sia la vittima/e e il presunto autore del reato sia maggiorenne, Procura Minorile: in caso il presunto autore del reato sia minorenni. Vi è anche l'obbligatorietà della segnalazione delle situazioni di pregiudizio a carico dei minori: L. 216/1991: per le situazioni di grave rischio l'istituzione scolastica è tenuta alla segnalazione delle medesime. Per pregiudizio si intende una condizione di rischio o grave difficoltà che provocano un danno reale o potenziale alla salute, alla sopravvivenza, allo sviluppo o alla dignità del bambino, nell'ambito di una relazione di responsabilità, fiducia o potere. La segnalazione come da procedura interna è il primo passo per aiutare un minore che vive una situazione di rischio o di grave difficoltà e va intesa come un momento di condivisione e solidarietà nei confronti del minore. La mancata segnalazione costituisce, infatti, omissione di atti d'ufficio (art.328 C.P.). Può essere utile, valutando accuratamente ciascuna situazione, attivare colloqui individuali con tutti i minori coinvolti, siano essi vittime, testimoni e/o autori. È importante considerare il possibile coinvolgimento dei genitori e di coloro incaricati della tutela dei minori coinvolti. L'intervento va indirizzato valutando l'eventuale impatto educativo e/o il contesto emotivo senza discriminare tra vittime, testimoni e/o autori.

Prevedere possibili incontri di mediazione tra i minori coinvolti vanno ponderati con la consapevolezza del loro stato emotivo, anche e in base agli elementi raccolti in merito del fatto/episodio avvenuto (elementi che si dovrebbero valutare di caso in caso). Importante è prevedere il coinvolgimento dei genitori sia della vittima che del bullo (ove possibile). Anche i genitori devono e possono segnalare casi di sospetto o evidenza dei fenomeni, segnalarlo al

Dirigente, o al docente coordinatore di classe o referente di istituto oppure direttamente al team antibullismo attraverso apposita procedura che definisce l'istituto (mail ad hoc, tramite gli uffici e postazioni specifiche, etc...). Gli insegnanti e i genitori, come studenti e studentesse, si possono rivolgere alla Helpline del progetto Generazioni Connesse, al numero gratuito 19696, attraverso la chat disponibile sul sito o tramite chat WhatsApp per ricevere supporto e consulenza. Per tutti i dettagli, il riferimento è agli allegati con le procedure

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.

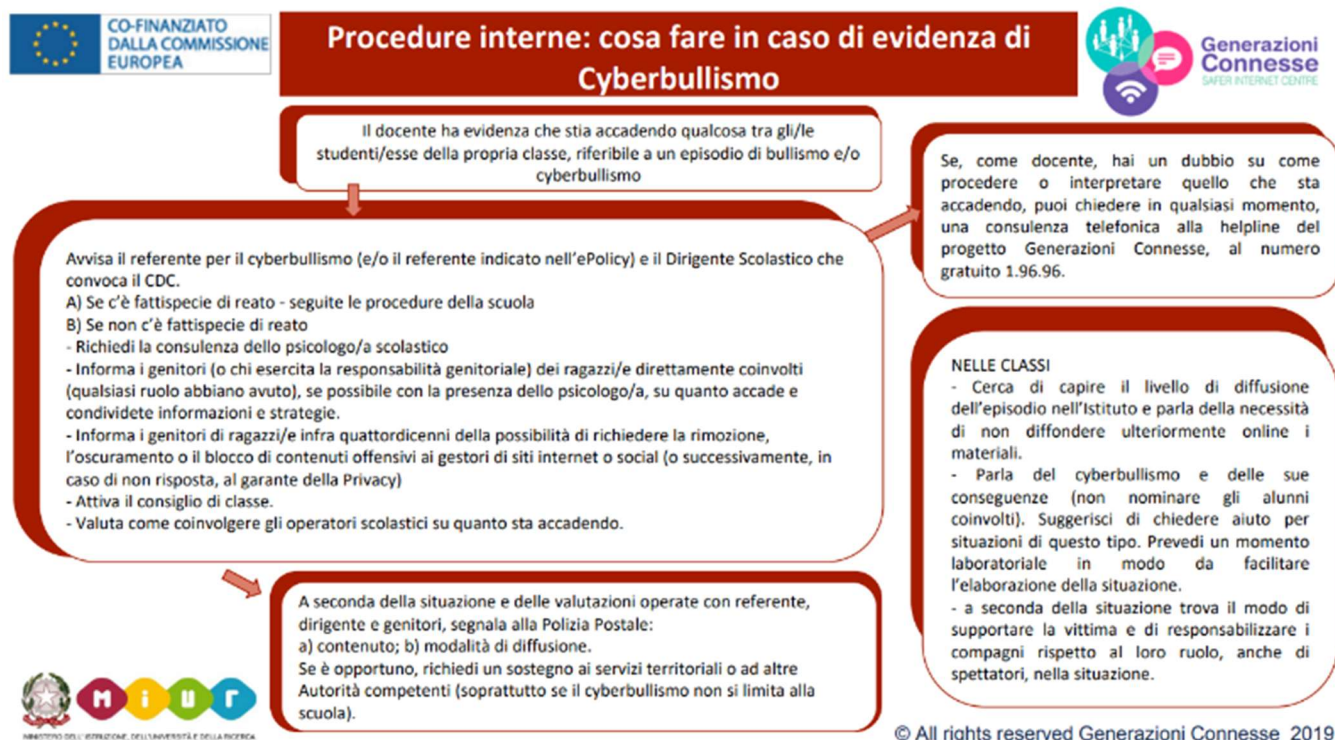
Aziende Sanitarie Locali: forniscono supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in Rete. In alcune regioni, come il Lazio e la Lombardia, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da Internet e alle situazioni di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

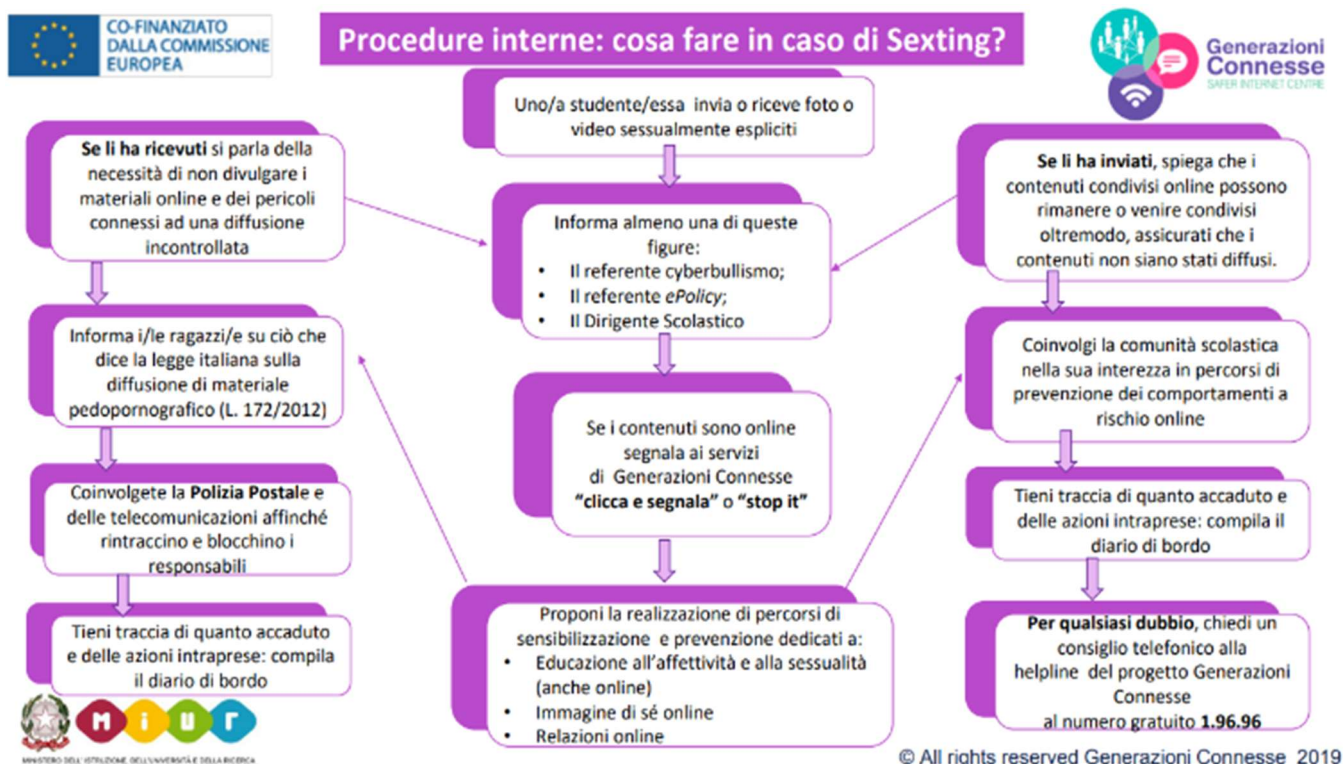
Tribunale per i Minorenni: segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

5.4. Allegati con le procedure

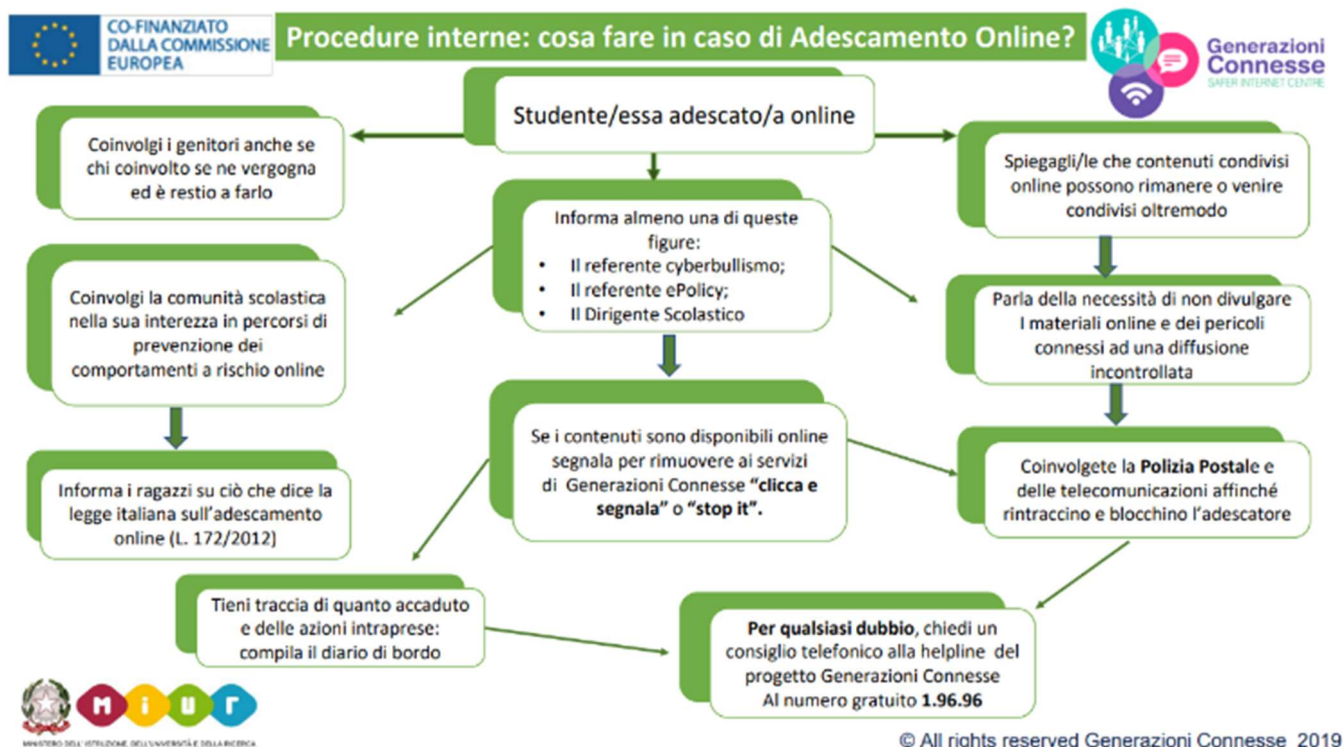
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



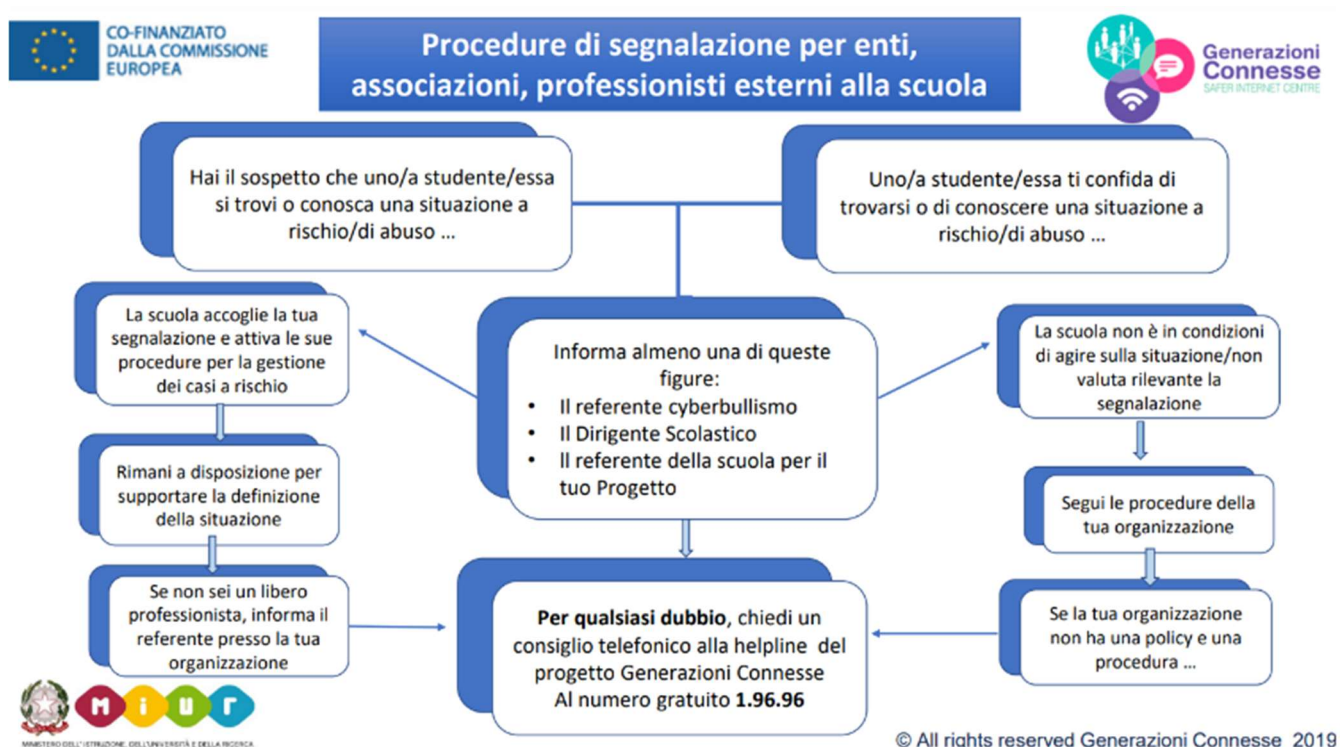
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



Procedure di segnalazione per enti, associazioni, professionisti esterni alla scuola



Il nostro piano d'azioni

Sulla base delle Linee Guida per l'uso positivo delle tecnologie digitali e della prevenzione dei rischi nelle scuole, vengono assunti i seguenti punti quali indicatori di co-costruzione tra scuola-famiglia-servizi territoriali, al fine di creare un modello composito e lineare di azioni condivise:

- coinvolgimento di tutti gli attori della scuola: alunni e alunne, docenti, genitori e personale ATA, per la realizzazione di una autentica comunità educante;
- alleanza educativa tra scuola e famiglia;
- interventi educativi ed azioni di supporto, quale prevenzione per eventuali comportamenti a rischio;
- misure preventive specifiche di tutela anche con l'ausilio di attori territoriali, come forze dell'ordine ed ASP per servizi specialistici;
- promozione dell'educazione al rispetto;
- sviluppo del pensiero critico;
- promozione dell'Educazione Civica Digitale.