

ISTITUTO OMNICOMPENSIVO - A. SACCO
Prot. 0008165 del 08/06/2026
I (Uscita)



Documento di ePolicy

A. SACCO

VIA G. FLORENZANO4 - 84037 - SANT'ARSENIO
Salerno (SA) - Campania
Data di approvazione: 08/06/2026 - 11:27

Cap 1 - Lo scopo della ePolicy

1.1 Scopo della ePolicy

Capitolo 1 - Presentazione dell'ePolicy

1. Scopo dell'ePolicy
2. Ruoli e responsabilità nell'implementazione dell'ePolicy
3. Integrazione dell'ePolicy con regolamenti e normativa generale esistenti
4. Condivisione e comunicazione dell'ePolicy all'intera comunità educante
5. I piani di Azione dell'ePolicy

Capitolo 2 - Sensibilizzazione e prevenzione

1. Sensibilizzazione e prevenzione
2. Il Curricolo Digitale
3. IL KIT DIDATTICO

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

1. Protezione dei dati personali e GDPR
2. Accesso ad Internet
3. Strumenti di comunicazione online (PUA)
4. Strumentazione personale (BYOD)

Capitolo 4 - 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

1.1 Scopo dell'ePolicy

(Questo paragrafo illustra lo scopo e gli obiettivi di questo documento programmatico per la cittadinanza digitale)

L' E-Policy ha come obiettivo principale quello di promuovere le competenze digitali per un uso delle tecnologie digitali positivo, critico e consapevole, da parte degli studenti e delle studentesse guidati dagli adulti coinvolti nel processo didattico-educativo.

La competenza digitale è una competenza chiave del cittadino europeo come indicato dal Consiglio Europeo

(Raccomandazione del 2018) che permette ad ogni cittadino di esercitare i propri diritti all'interno degli ambienti digitali (ONU - [Commento Generale 25](#): I diritti dei minori negli ambienti digitali).

L'ePolicy è un documento programmatico che permette di lavorare su quattro obiettivi:

1. Il piano di azioni triennale per promuovere nell'intera comunità scolastica l'uso sicuro responsabile e positivo della rete;
2. le misure per la prevenzione e la sensibilizzazione di comportamenti on-line a rischio;
3. le norme comportamentali e le procedure di utilizzo delle Tecnologie dell'Informazione e della Comunicazione (ICT) in ambiente scolastico;
4. le misure per la rilevazione, segnalazione e gestione delle situazioni rischiose legate ad un uso non corretto delle tecnologie digitali.

A partire dall'anno scolastico 2025/26, l'I.O.C. "A. Sacco" di Sant'Arsenio ha aderito al progetto Safer Internet Centre - Generazioni Connesse, coordinato dal Ministero dell'Istruzione e del Merito e co-finanziato dall'Unione Europea, per elaborare questo documento di E-policy. L'obiettivo prefissato è quello di educare e sensibilizzare tutta la comunità scolastica, alunni/e, insegnanti e genitori all'uso sicuro e consapevole delle tecnologie digitali e della rete.

Nello specifico, attraverso l'Epolicy, il nostro Istituto si prefigge di promuovere:

- l'utilizzo consapevole, critico e sicuro delle tecnologie digitali e di Internet da parte di tutti i soggetti coinvolti nel processo educativo (docenti, personale scolastico, famiglie ed alunni);
- la prevenzione dei rischi online legati all'uso non responsabile delle tecnologie attraverso l'adozione di norme comportamentali e procedure;
- la gestione delle emergenze fornendo protocolli chiari su come rilevare, segnalare e gestire eventuali episodi di bullismo, cyberbullismo o uso improprio delle tecnologie.
- la collaborazione tra scuola e famiglie per diffondere nei giovani una cultura digitale sicura non solo nell'ambiente scolastico ma nella vita quotidiana.

Il documento è stato stilato nel corso del secondo quadrimestre dai componenti del Team Antibullismo e dell'Emergenza composto dal Dirigente Scolastico, dal Referente per il Bullismo e Cyberbullismo, dall'Animatore Digitale, dai componenti del Team Digitale e dai Referenti per l'Inclusione che rappresentano ogni grado scolastico dell'Istituto: infanzia, primaria, secondaria di primo grado e secondaria di secondo grado.

Riferimenti normativi

La ePolicy tiene conto delle principali disposizioni legislative, quali:

- Legge 107/2015 sullo sviluppo delle competenze digitali degli studenti;
- Regolamento UE 2016/679 (GDPR) per la protezione dei dati personali;
- Legge 71/2017 sulla tutela dei minori per la prevenzione e il contrasto al bullismo e cyberbullismo;
- Legge 92/2019 sulla introduzione nel sistema scolastico dell'Educazione Civica;
- Linee di Orientamento per il contrasto dei fenomeni di Bullismo e Cyberbullismo del 2021 (D.M.18 del 2021);
- Legge 70/2024 e Decreto Legislativo 99/2025 sulla prevenzione e il contrasto del bullismo e del cyberbullismo;

- Altre norme pertinenti in ambito scolastico e digitale.

1.2 - ePolicy: ruoli e responsabilità nell'implementazione dell'ePolicy

- (In questo paragrafo vengono dettagliati ruoli e responsabilità nell'implementazione del documento all'interno dei contesti scolastici ivi inclusi rappresentanti genitori e studenti per secondaria II grado).

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

È opportuno che nel documento vengano definiti con chiarezza ruoli, compiti e responsabilità di ciascuna delle figure all'interno dell'Istituto.

In questo paragrafo dell'ePolicy è importante specificare le figure professionali che, a vario titolo, si occupano di gestione e programmazione delle attività formative, didattiche ed educative dell'Istituto e tutte quelle figure appartenenti alla comunità educante.

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 ed inserendola nelle misure di sicurezza più generali dell'intero Istituto;
- ha la responsabilità di fornire sistemi per un uso sicuro delle TIC, internet, i suoi strumenti ed 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;
- deve 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;
- deve essere a conoscenza delle procedure da seguire in caso di un grave incidente di sicurezza online;
- deve garantire adeguate valutazioni di rischio nell'usare strumenti e TIC, effettuate in modo che comunque quanto programmato possa soddisfare le istanze educative e didattiche dichiarate nel PTOF di Istituto;
- deve garantire l'esistenza di un sistema che assicuri il monitoraggio e il controllo interno della sicurezza online in collaborazione con le figure di sistema;
- deve essere a conoscenza ed attuare le procedure necessarie in caso di grave incidente di sicurezza online.

L'ANIMATORE DIGITALE E IL TEAM PER L'INNOVAZIONE DIGITALE

L'animatore digitale e il Team per l'Innovazione digitale sono co-responsabili, con il referente ePolicy, dell'attuazione dei piani di azione in particolare in riferimento alla formazione dei docenti. Sono inoltre responsabili del controllo all'accesso da parte degli studenti delle Tic

IL REFERENTE PER IL BULLISMO E CYBERBULLISMO

Il referente cyberbullismo è co-responsabile, con il team ePolicy, dell'attuazione dei piani di azione e coordina le iniziative di prevenzione e contrasto del cyberbullismo.

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 ha le funzioni di coadiuvare il Dirigente Scolastico, coordinatore del Team nella scuola, 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.

Il Team ha il compito di:

- coadiuvare il Dirigente scolastico, coordinatore del Team, nella definizione degli interventi di prevenzione del bullismo (per questa funzione partecipano anche il presidente del Consiglio d'Istituto e i Rappresentanti degli studenti).
- Intervenire (come gruppo ristretto, composto da Dirigente e referente o referenti per il bullismo e il cyberbullismo, psicologo o pedagogo, se presente) nelle situazioni acute di bullismo.
- Promuovere la redazione e l'applicazione della ePolicy e monitorare le segnalazioni.

I/LE DOCENTI

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 LIM 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 senza averne prima parlato con i genitori. 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 altresì regolarmente i comportamenti a rischio (sia dei potenziali bulli, sia delle potenziali vittime) e hanno il dovere morale e professionale di segnalare al Dirigente Scolastico 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.

RESPONSABILE DELLA PROTEZIONE DEI DATI

Il Responsabile della protezione dei dati (RPD o 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 E AUSILIARIO (ATA)

Il personale ATA, all'interno dei singoli regolamenti d'Istituto, è coinvolto nelle pratiche di prevenzione - ivi incluso il processo di definizione e implementazione dell'ePolicy di Istituto - ed è tenuto alla segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo.

GLI STUDENTI E LE STUDENTESSE

Gli studenti e le studentesse devono, in relazione al proprio grado di maturità e consapevolezza raggiunta, utilizzare al meglio le tecnologie digitali in coerenza con quanto richiesto dai docenti. Con il supporto della scuola dovrebbero imparare a tutelarsi online, tutelare i/le propri/e compagni/e e rispettarli/le. Affinché questo accada devono partecipare attivamente a progetti ed attività che riguardano l'uso positivo delle TIC e della Rete e farsi promotori di quanto appreso anche attraverso possibili percorsi di peer education.

I rappresentanti degli/delle studenti sono informati del documento di ePolicy e invitati a costruire i piani di azione, a partire dal secondo anno della secondaria di II grado,

I GENITORI/ADULTI DI RIFERIMENTO

I Genitori, in continuità con l'Istituto scolastico, sono attori partecipi e attivi nelle attività 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 ESTERNI PUBBLICI E PRIVATI E LE ASSOCIAZIONI

Enti esterni pubblici e privati, il mondo dell'associazionismo dovranno conformarsi alla politica della scuola riguardo all'uso consapevole delle TIC e della rete per la realizzazione di iniziative nelle scuole, finalizzate a promuovere un uso positivo e consapevole delle Tecnologie Digitali da parte dei più giovani, e/o finalizzate a prevenire e contrastare situazioni di rischio online e valutare la rispondenza delle proposte di attività di sensibilizzazione/formazione alle esigenze di qualità contenute nel documento di ePolicy. Dovranno inoltre promuovere comportamenti sicuri durante le attività che si svolgono con gli/le studenti e verificare di aver implementato una serie di misure volte a garantire la tutela dei minori nel caso di insorgenza di problematiche e ad assicurarne la tempestiva individuazione e presa in carico.

Alla luce di tutto ciò emerge il ruolo chiave che spetta all'intera comunità scolastica nell'educare gli studenti al rispetto delle norme, dei diritti e della privacy, contribuendo in tal modo a prevenire situazioni di rischio e a diffondere un approccio consapevole alla tecnologia.

1.3 Integrazione ePolicy nei documenti scolastici

(Il paragrafo spiega in che modo integrare il documento nel Regolamento dell'Istituto Scolastico da aggiornare con specifici riferimenti all'E-policy, così come nel RAV e all'interno del Patto di Corresponsabilità, in coerenza con le Linee Guida Miur e le indicazioni normative generali sui temi in oggetto).

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.

Il Regolamento di Istituto viene aggiornato alla luce della presente ePolicy; allo stesso modo il Patto di corresponsabilità. Relativamente al PTOF elaborato dal nostro Istituto per il triennio 2025-2028, si specifica che esso include alcune progettualità ed iniziative già consolidate negli anni sul tema della prevenzione al bullismo e al cyberbullismo e più in generale al benessere psico-fisico degli studenti (sportello di ascolto per studenti, cineforum, teatro, incontri con associazioni, iniziative didattiche dedicate). In sede di aggiornamento del PTOF previsto per l'anno scolastico 2026/2027 si provvederà inoltre ad inserire il documento di ePolicy d'Istituto e i progetti formativi messi a disposizione dalla piattaforma Generazioni Connesse, rivolti a famiglie, docenti e studenti.

1.4 Condivisione e comunicazione dell'ePolicy

Il paragrafo dettaglia i seguenti aspetti:

1. il curriculum sulle competenze digitali per la comunità educante (il DigComp2.2);
2. Informazione della comunità educante (in particolare le famiglie) sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali con relative informative;
3. 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).

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.

Strategie per la diffusione del documento ePolicy

Nello specifico, l'I.O.C. "A. Sacco" prevede di utilizzare le seguenti strategie al fine di condividere e comunicare il presente documento all'interno della comunità scolastica e del territorio di appartenenza:

- Sito Web Istituzionale: l'ePolicy completa, dopo essere stata approvata dal Collegio dei Docenti, sarà pubblicata in una sezione dedicata del sito dell'Istituto;
 - Incontri Informativi: la scuola organizzerà incontri dedicati per presentare l'ePolicy secondo le seguenti modalità:
 - Docenti: in sede di Collegio dei Docenti
 - ATA: condivisione del documento che verrà esposto in versione semplificata negli spazi dell'Istituto (bacheche e segreteria)
 - Studenti: lettura in classe durante le attività di Educazione Civica e dell'Orientamento
 - Genitori: condivisione all'inizio dell'anno scolastico del Patto di Corresponsabilità aggiornato con specifici riferimenti all'ePolicy
 - Protocolli d'Intesa: ogni accordo di collaborazione richiederà esplicitamente l'adesione alla presente ePolicy.
-

1.5 - I Piani di Azione 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 che 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 sui temi dell'educazione civica digitale e dell'utilizzo sicuro e consapevole delle tecnologie e della rete:

- la rilevazione dei bisogni
- le iniziative informative e formative,
- la formazione di docenti, studenti e studentesse, e famiglie,
- il monitoraggio e la valutazione delle azioni (laddove possibile, anche all'interno del RAV);

I Piani di Azione si distinguono tra standard, comuni ad 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 dell'Istituto dedicato alle famiglie ed a studenti/esse;
- Diffondere l'ePolicy negli ambienti scolastici, a studenti e studentesse, docenti e famiglie attraverso le versioni friendly dell'ePolicy;

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;

MODULO III

- Integrare l'ePolicy (norme, regolamenti e procedure) nei documenti dell'Istituto;
- Aggiornare la Politica d'Uso Accettabile (PUA) della scuola ed il regolamento BYOD dell'Istituto;

MODULO IV

- 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.

2° 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

IL NOSTRO PIANO D'AZIONI

Al fine di consentire un'efficace implementazione dell'ePolicy in linea con le esigenze della comunità scolastica l'Istituto "A. Sacco" pianifica una serie di azioni e attività da completare entro ogni annualità scolastica.

1. AZIONI DA SVOLGERE

Attività a breve termine (entro un anno scolastico):

- Valutazione delle competenze: analizzare il fabbisogno formativo degli studenti e dei docenti in merito alle competenze digitali e all'integrazione delle TIC nella didattica
- Sensibilizzazione: organizzare un evento di presentazione del progetto "Generazioni Connesse" per studenti, docenti e genitori

Attività a medio termine (entro i prossimi tre anni):

- Formazione continua: organizzare e promuovere corsi di formazione per i docenti sull'uso e l'integrazione delle TIC e dell'Intelligenza Artificiale (IA) nella didattica
- Coinvolgimento della comunità: organizzare incontri con esperti di competenze digitali, aperti a docenti, studenti e genitori

2. MONITORAGGIO E AGGIORNAMENTO DELL'EPOICY

Monitoraggio dell'implementazione della ePolicy:

- Rilevazioni periodiche per conoscere interessi, comportamenti, abitudini ed esigenze formative della popolazione scolastica
- Monitoraggio delle attività curriculari svolte nelle classi nell'ambito del Curricolo di educazione Civica

Aggiornamento del documento:

- L' ePolicy verrà aggiornata periodicamente e quando si verificheranno cambiamenti significativi in riferimento all'uso delle tecnologie digitali all'interno della scuola.

Il monitoraggio e la revisione del documento E-policy viene affidato al docente Referente del Bullismo e Cyberbullismo, coadiuvato dal gruppo di lavoro, con la partecipazione dell'animatore digitale. Le modifiche del documento saranno discusse con tutti i membri del personale docente. Il processo di valutazione sarà condotto annualmente e la valutazione al termine del percorso triennale costituirà il punto di partenza per l'aggiornamento del prossimo documento.

Si evidenzia che l'Istituto "Sacco" partecipa dall'anno scorso al "Monitoraggio nazionale sui fenomeni del bullismo e cyberbullismo" coordinato dal Ministero dell'Istruzione e del Merito (MIM) tramite la Piattaforma ELISA, in collaborazione con l'Università di Firenze.

3. FORMAZIONE

- Avviare l'utilizzo del corso online di Generazioni Connesse per docenti, ATA, studenti e famiglie
- Realizzare corsi di formazione su base volontaria rivolti al personale scolastico e agli studenti
- Promuovere il corso online di Generazioni Connesse valido ai fini della Formazione Scuola lavoro e dell'Orientamento per le classi del Triennio
- Avviare l'introduzione del kit didattico come metodo e risorsa di lavoro in alcune classi pilota

Nel corrente anno scolastico sono stati attivati con i fondi PNRR dei percorsi destinati alla formazione del personale scolastico sulla transizione digitale che hanno coinvolto tutti i gradi dell'Istituto. Il progetto "Insieme digitalizziamoci" è stato così declinato:

- Corso sulle UDA
- Corso sul Curricolo Verticale di Istituto
- Corso sui BES.

1.6 - Le risorse di Generazioni Connesse

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](#)

Per lo sviluppo di attività didattiche e per la formazione della comunità scolastica l'I.O.C. "A.Sacco" utilizzerà i seguenti strumenti tra quelli offerti da Generazioni Connesse:

- Kit Didattico
- Area formazione (per docenti, famiglie, studenti/sse con ePolicy)
- Canale Youtube (webinar, video-stimolo, serie per target).

Cap 2 - Sensibilizzazione e prevenzione

2.1 - Sensibilizzazione e prevenzione

(Il 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.

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.

Al fine di ridurre l'incidenza di situazioni di rischio il nostro Istituto promuove interventi sia di sensibilizzazione che di prevenzione da attuare attraverso l'organizzazione di strategie didattiche inclusive e l'integrazione con la rete dei servizi territoriali locali (Polizia postale, Associazioni territoriali, ASL, USR).

Il primo step da perseguire è l'implementazione della competenza digitale in tutti gli alunni in modo da formare e consolidare quelle competenze educative di base necessarie per poter gestire la navigazione in rete. Un ruolo cruciale può essere svolto dall'insegnamento dell'Educazione Civica, proprio per la sua trasversalità a tutte le discipline.

Il Curricolo di Educazione Civica - nucleo concettuale Cittadinanza Digitale - si propone infatti di promuovere un uso etico e consapevole delle tecnologie digitali. L'obiettivo è aiutare gli studenti a riflettere in modo critico su ciò che condividono online, valutando con attenzione la diffusione di dati e notizie in rete e sviluppando una maggiore sensibilità verso i temi della privacy e della tutela dell'identità personale (competenza n.10 e n.12). La strutturazione in UDA dedicate del percorso mira inoltre a educare i discenti all'uso responsabile dei dispositivi elettronici, sottolineando come le tecnologie debbano essere uno strumento utile per arricchire e integrare le loro competenze senza mai sostituirle.

AZIONI DEL NOSTRO ISTITUTO

- Nomina del Referente del bullismo e cyberbullismo in ogni grado dell'Istituto, che coordina le varie azioni nei rispettivi ordini di scuola dell'Omnicomprendivo;
- Iniziative didattiche di sensibilizzazione attraverso lavori predisposti dagli alunni (disegni, poesie, testi, rappresentazioni teatrali, prodotti multimediali, giochi interattivi) da condividere con la comunità scolastica, genitori e territorio di appartenenza in occasione di giornate dedicate:
 - Giornata della gentilezza (13 Novembre)
 - Giornata Internazionale dei diritti dell'infanzia e dell'adolescenza (20 Novembre)
 - Giornata Internazionale sulla violenza di genere (25 Novembre)
 - Giornata del rispetto (20 gennaio)
 - Giornata nazionale contro il bullismo e cyberbullismo (7 Febbraio)
 - Safer Internet Day - Giornata mondiale per la sicurezza in Rete

- Iniziative con la collaborazione di Enti e Associazioni del territorio;
- Incontri con la Polizia Postale, Polizia di Stato e Arma dei Carabinieri;
- Sportello d'ascolto con psicologo;
- Diffusione di buone pratiche.

Nel corrente anno scolastico l'Istituto "Sacco" ha aderito alle seguenti iniziative:

- Percorso - "Valorizzazione e diffusione delle pari opportunità, dell'educazione affettiva e della gestione delle emozioni" promosso dalla Regione Campania
- Percorso - "Educazione alla legalità" promosso dall'Associazione Italiana Giovani avvocati (AIGA) della sezione di Lagonegro (PZ)
- Percorso - "Star Bene insieme" promosso dall'ASL di Salerno.

2.2 - Il Curricolo Digitale

Per realizzare questo obiettivo l'istituto utilizza le risorse messe a disposizione a livello nazionale e internazionale.

Il DigComp 2.2, framework europeo sulle competenze digitali, permette di costruire una cornice precisa in cui inquadrare i temi e le corrispondenti competenze da proporre nell'Istituto non solo per gli studenti.

Al suo interno vengono identificati alcuni temi sui quali è costruita una proposta specifica per le famiglie e gli studenti (formazione). Tale cornice trova poi sviluppo specifico, per gli studenti, nel curriculum di educazione alla Cittadinanza Digitale previsto dalla L. 92/2019. Il curriculum prende forma attorno all'ePolicy e le attività didattiche sono legate al documento ed alle scelte dell'Istituto al suo interno.

Nel curriculum va previsto in ogni classe un appuntamento didattico specifico, calibrato sull'età degli alunni, e l'utilizzo dei kit didattici per favorire da parte degli studenti una maggiore conoscenza e consapevolezza delle finalità del presente documento.

I regolamenti e le attività sviluppate sul tema della prevenzione presenti nell'ePolicy sono parte, costante ma non esclusiva, delle azioni di disseminazione e sensibilizzazione descritte ed attuate dall'Istituto.

Il nostro Istituto realizza dei percorsi interdisciplinari volti a promuovere il corretto utilizzo delle tecnologie dell'informazione e della comunicazione (TIC) in coerenza con gli obiettivi previsti nel Curriculum di Educazione Civica, aggiornato secondo le nuove Linee Guida per l'insegnamento dell'educazione civica DM 183/2024 e disponibile sul sito web istituzionale.

2.3 - Il Kit Didattico

L'ePolicy prevede, a livello macro, un lavoro di lettura e d'intenti condivisi dall'intera comunità scolastica, a livello micro,

invece, immagina che la singola classe lavori anche su tematiche direttamente collegate alla sicurezza in rete, ma complesse e di non immediata ricaduta nelle programmazioni scolastiche (etica e digitale, algoritmi, datafication). A tal fine si è progettato e predisposto del materiale che possa funzionare sia da attivatore, sia d'accompagnamento ai docenti e agli studenti nella fase più delicata ed incisiva del processo di prevenzione: la lezione in classe.

Pertanto, il progetto Generazioni Connesse, a supporto del lavoro dell'e-Policy ha previsto per i docenti e studenti di ogni segmento scolare un nuovo [Kit Didattico](#) che contiene materiali per le lezioni e per il proprio aggiornamento, a partire dalla scuola d'infanzia fino alla secondaria di secondo grado. Il Kit può essere usato nella sua interezza oppure può essere oggetto di selezione e scelta, sulla base di quanto fatto dal docente.

Il kit include schede didattiche differenziate per i vari ordini di scuola e "pillole" teoriche per la formazione interna del personale. La sua struttura si allinea al modello ICF-CY, che garantisce un approccio inclusivo e accessibile per tutti, in linea con la missione educativa della nostra scuola.

Integrare questo kit nella nostra ePolicy significa pertanto non solo promuovere la sicurezza in rete, ma anche il benessere digitale e l'autonomia critica degli alunni.

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

3.1 - Protezione dei dati personali e GDPR

La protezione dei dati personali delle persone fisiche costituisce un diritto fondamentale. L'art. 8, par. 1, della Carta dei diritti fondamentali dell'Unione europea e l'art. 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. Le principali normative di riferimento sono il Regolamento Generale sulla Protezione dei Dati 2016/679 noto anche come GDPR, e il Dlgs 196/2003 conosciuto come Codice Privacy.

Il settore dell'istruzione è particolarmente impattato dalla tematica privacy in considerazione del fatto che gli Istituti Scolastici sono chiamati, necessariamente, a trattare un'enorme mole di dati personali.

Con l'entrata in vigore del GDPR è stato introdotto l'obbligo per ciascun Istituto scolastico di provvedere alla designazione di un Responsabile della protezione dei dati personali (RPD o DPO).

I principali obblighi in materia di protezione dei dati personali consistono nella definizione di un "organigramma privacy", nel rilascio dell'informativa al momento della raccolta dei dati e nella tenuta di un registro dei trattamenti.

In merito, l'I.O.C. "A. Sacco" ha adeguato tutta la modulistica al Regolamento UE 2016/679 (GDPR) e al D.Lgs. 30 giugno 2003 n.196 ("Codice in materia di protezione dei dati personali", come modificato dal D.Lgs. 101/2018).

Sul sito dell'istituto sono presenti i documenti redatti e validi in relazione alle normative di tutti i sistemi on line utilizzati in Istituto: <https://www.iis-sacco.edu.it/>

È presente, come d'obbligo, una apposita sezione per i documenti relativi:

- al trattamento dei dati personali accessibile alla pagina

<https://www.iis-sacco.edu.it/privacy-policy/>

- al GDPR consultabili al seguente link

<https://www.iis-sacco.edu.it/documento/regolamenti/#668-668-regolamenti-p1>

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.

Il nostro Istituto ha adottato il Regolamento di Politica di Uso Accettabile (PUA) delle Tecnologie Digitali e della Rete Internet, consultabile al seguente indirizzo:

<https://www.iis-sacco.edu.it/documento/regolamenti/#:~:text=Download-,E%2DPolicy,-3.82%20MB>

3.3 - BYOD

La presente ePolicy conterrà 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 infatti 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.

Strumenti di comunicazione online utilizzati a scuola

Fra gli strumenti di comunicazione troviamo:

1. Sito Web della scuola raggiungibile all'indirizzo (<https://www.iis-sacco.edu.it/>), utilizzato per fornire informazioni di servizio rivolte ad alunni/e e genitori a integrazione delle comunicazioni, circolari e avvisi trasmessi mediante il Registro Elettronico e per trasmettere all'esterno l'identità, i valori, le azioni, i progetti e l'idea di educazione che l'Istituto porta avanti;
2. **Registro Elettronico** – piattaforma Argo con tutte le sue funzionalità: utilizzato per facilitare e rendere più partecipata la didattica e la comunicazione scuola-famiglia;
3. **Piattaforma Google Workspace for Education** (in via di implementazione), con le sue app incluse: e-mail, drive, meet, classroom, etc.). Ad ogni docente e alunno/a sarà assegnato un indirizzo e-mail istituzionale (.....@iis-sacco.edu.it) utilizzato per scopi didattici.

Per ciò che concerne la gestione degli strumenti personali (cellulari, tablet, pc) da parte di alunni/e, docenti, personale scolastico e ogni altro operatore presente a qualsiasi titolo nella scuola si fa riferimento a quanto riportato nel Patto di Corresponsabilità e nel Regolamento di Istituto.

Cap 4 - Segnalazione e gestione dei casi

4.1 - Cosa Segnalare

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. Queste, inoltre, forniscono valide indicazioni anche per i professionisti e le organizzazioni esterne che operano con la scuola.

Nelle procedure sono indicate le figure preposte all'accoglienza della segnalazione e alla presa in carico e gestione del caso, nonché le modalità di coinvolgimento del Dirigente Scolastico e del Referente per il contrasto al bullismo e al cyberbullismo. 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. 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 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, per quanto possibile, la rimozione del materiale on-line e il blocco della sua diffusione per mezzo dei 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.

COSA SEGNALARE

Si considerano da segnalare tutti quei contenuti che, anche se non esplicitamente denunciati come atti di bullismo, cyberbullismo o violenza, mettono in allarme il docente e il personale della scuola.

A titolo esemplificativo, rientrano in questa categoria:

- Contenuti relativi alla violazione della privacy, come la diffusione non autorizzata di immagini, video o informazioni personali di coetanei, anche tramite social network, chat o piattaforme di messaggistica istantanea.
- Contenuti relativi all'aggressività o alla violenza, come minacce, insulti, denigrazione, esclusione sistematica, incitamento all'odio (hate speech) o alla discriminazione, sia in presenza che online.
- Contenuti relativi alla sessualità, come la condivisione o ricezione di immagini intime o sessualmente esplicite (sexting), richieste inappropriate da parte di adulti o coetanei (adescamento), commenti a sfondo sessuale, o espressioni che evidenziano disagio, pressione o mancanza di consapevolezza rispetto alla propria sfera sessuale.

MISURE SANZIONATORIE

La scuola gestirà i casi sopra rilevati privilegiando azioni educative e correttive.

La sanzione verrà differenziata a seconda della gravità del comportamento e delle conseguenze che da esso derivano: è sempre opportuna la condivisione a livello di Consiglio di Classe/Team di Docenti di ogni episodio rilevato.

Alcuni avvenimenti di lieve rilevanza possono essere affrontati e risolti con la discussione collettiva in classe o assegnazione di attività aggiuntive da svolgere a casa sui temi di Cittadinanza e Costituzione.

Altri casi di rilevanza maggiore (ad esempio insulti occasionali in chat, invio di immagini improprie) verranno segnalati al Referente del Bullismo e Cyberbullismo e poi al Dirigente Scolastico, il quale potrà affrontarli convocando genitori e alunni/e, alla presenza di tutti gli attori in campo, per riflettere insieme sull'accaduto e individuare strategie comuni d'intervento.

Nei casi più gravi (ad esempio sexting, grooming) è necessario informare il Dirigente Scolastico che, nel caso di reati veri e propri, effettuerà la denuncia all'autorità giudiziaria.

Tutte le segnalazioni dei docenti devono essere messe a verbale e protocollate.

L'ITER CONSIGLIATO

"In generale, in caso di episodio sospetto e/o denunciato, si suggerisce di seguire il seguente schema di intervento come da **Linee di orientamento per la prevenzione e il contrasto dei fenomeni di Bullismo e Cyberbullismo, 2017**:

- colloquio individuale con la vittima o colloqui individuali con le singole vittime;
- colloquio individuale con il bullo o colloqui individuali con i singoli bulli;
- possibile colloquio con i bulli insieme (in caso di gruppo);
- possibile colloquio con vittima/e e bullo/i se le condizioni di consapevolezza lo consentono;
- coinvolgimento dei genitori di vittima/e e bullo/i.

Tuttavia, essendo ogni situazione di bullismo differente in termini di modalità, è opportuno valutare di volta in volta quale sia l'ordine più efficace.

Si ricorda che, in base alle norme vigenti:

- in caso di rilevanza penale del comportamento è obbligo della scuola segnalare l'evento all'autorità giudiziaria;
- in caso di segnalazione di episodi cyberbullismo, il dirigente scolastico ha l'obbligo di informare tempestivamente la famiglia della vittima come indicato nella L.71/2017."

Per ulteriori dettagli si rimanda agli allegati con le procedure e alla tabella delle sanzioni disciplinari per la gestione di atti di bullismo o di cyberbullismo acclusa al presente documento.

4.2 - 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.

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.

Strumenti a disposizione di studenti/esse

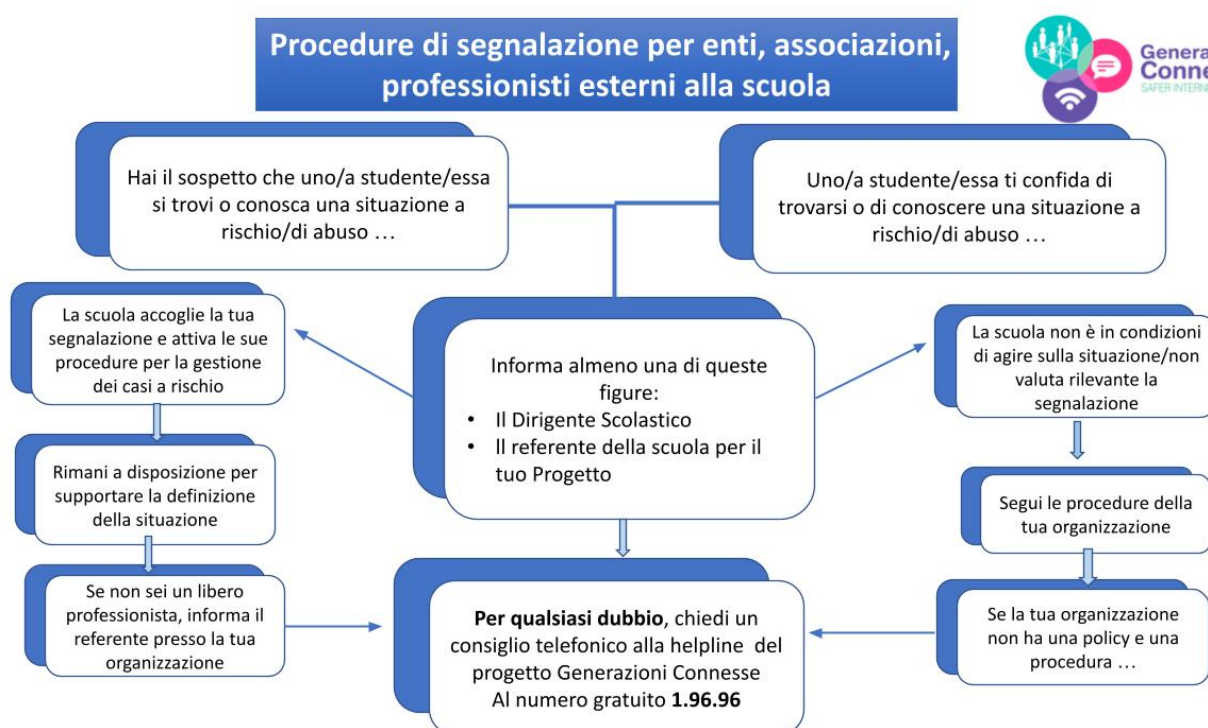
Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione: un indirizzo e-mail specifico per le segnalazioni; scatola/box per la raccolta di segnalazioni anonime da inserire in uno spazio accessibile e ben visibile della scuola; sportello di ascolto con professionisti; docente referente per le segnalazioni.

In particolare, sarebbe utile che la scuola attivi un sistema di segnalazione utile anche al monitoraggio dei fenomeni dal quale partire per integrare azioni didattiche preventive e giornate di sensibilizzazione, insieme agli Enti/Servizi presenti sul territorio di riferimento. Importante, altresì, immaginare e programmare percorsi di peer education per la prevenzione e il

contrasto degli agiti.

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.

Procedure



Procedure interne: cosa fare in caso di evidenza di Cyberbullismo



Il docente ha evidenza che stia accadendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo

Se non è già stato fatto, avvisa il referente per il cyberbullismo (e/o il team antibullismo) che attiva le procedure ("Corso 4" della piattaforma ELISA) e il Dirigente Scolastico.

Ricordare sempre che in base alla legge 71-2017:

A) Se c'è fattispecie di reato va fatta la segnalazione alle forze dell'ordine

B) Se non c'è fattispecie di reato.

Il DS (e/o il team antibullismo):

- informa i genitori (o chi esercita la responsabilità genitoriale) dei ragazzi/e direttamente coinvolti (qualsiasi ruolo abbiano avuto) su quanto accade e condivide informazioni e strategie.
- Informa i genitori di ragazzi/e infra quattordicenni della possibilità di richiedere la rimozione, l'oscuramento o il blocco di contenuti offensivi ai gestori di siti internet o social (o successivamente, in caso di non risposta, al garante della Privacy)
- Attiva il consiglio di classe.

Se, come docente, hai un dubbio su come procedere o interpretare quello che sta accadendo, puoi chiedere in qualsiasi momento, una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

NELLE CLASSI

Il team antibullismo collabora coi docenti della classe per realizzare l'intervento nella classe:

a seconda della situazione valuta se

- affrontare direttamente l'accaduto o
- sensibilizzare la classe (vedi Corso 4 Piattaforma Elisa)
- trova il modo di supportare la vittima e di responsabilizzare i compagni rispetto al loro ruolo, anche di spettatori, nella situazione.

A seconda della situazione e delle valutazioni operate con referente, dirigente e genitori, segnala alla Polizia Postale:

a) contenuto; b) modalità di diffusione.

Se è opportuno, richiedi un sostegno ai servizi territoriali o ad altre Autorità competenti (soprattutto se il cyberbullismo non si limita alla scuola).

Procedure interne: cosa fare in caso di sospetto di Cyberbullismo



Il docente riceve una segnalazione (da un genitore, un altro studente ...) o sospetta che stia accadendo qualcosa a uno/a studente/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo

Ricorda agli studenti che possono segnalare al gestore del sito/social e al garante privacy eventuali contenuti offensivi/lesivi che li riguardano

Condividi con il referente o al team antibullismo: si attiva il processo di attenzione e valutazione a cura del referente.

Insieme si valuta se è il caso

- di avvisare il consiglio di classe;
- di avvisare il Dirigente Scolastico, anche in base al regolamento interno o a prassi consolidate.

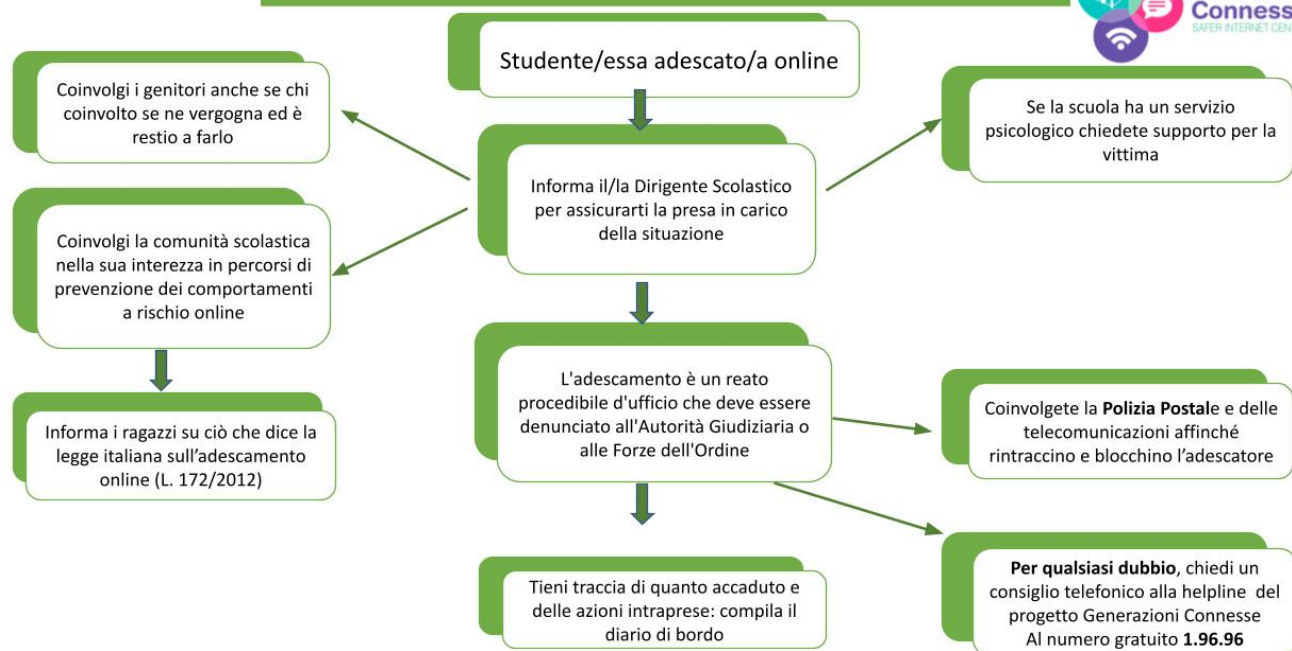
Se, come docente, hai un dubbio su come procedere o interpretare quello che sta accadendo, puoi chiedere in qualsiasi momento, una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

Scarica le linee di orientamento per la prevenzione e il contrasto dei fenomeni di bullismo e cyberbullismo

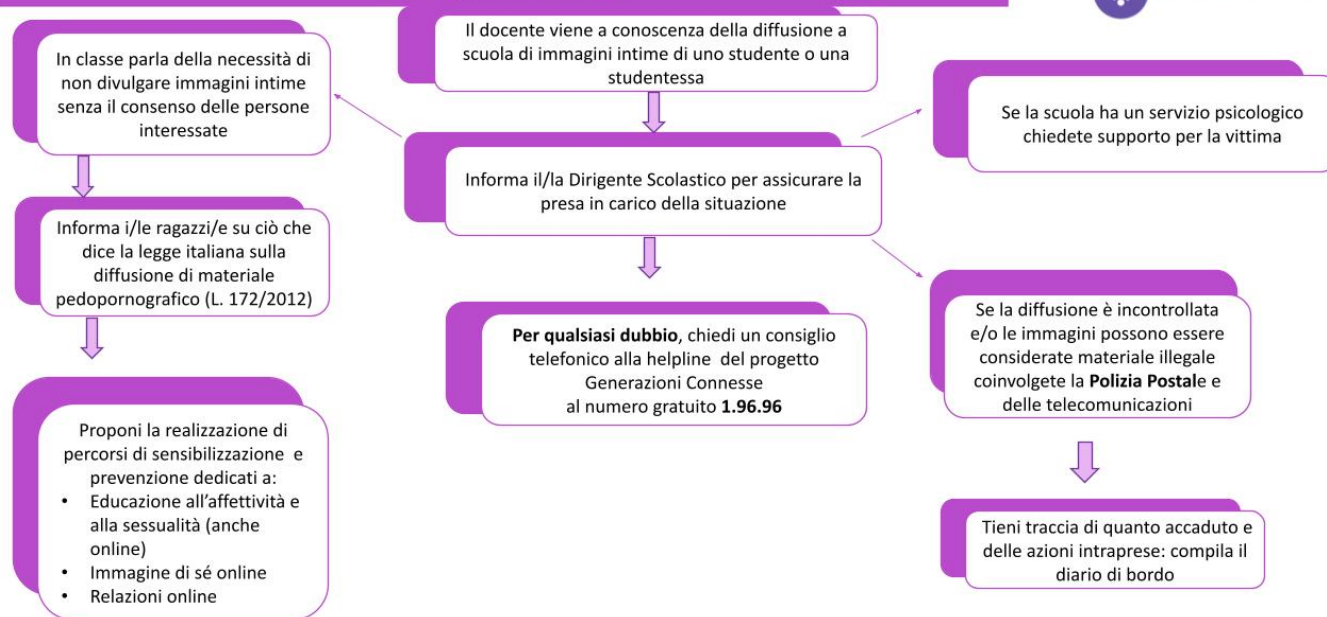
Se emergono evidenze passa allo schema successivo

Ricorda a studenti/esse che possono chiedere in qualsiasi momento una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96 o via chat

Procedure interne: cosa fare in caso di Adescamento Online?



Procedure interne: cosa fare in caso di diffusione non consensuale di immagini intime?



STRUMENTI E LINEE DI INTERVENTO

I docenti, gli alunni, le famiglie e tutto il personale che opera presso il nostro Istituto possono segnalare al Referente del Cyberbullismo e al Team Antibullismo casi sospetti o evidenti di bullismo, cyberbullismo, sexting, adescamento online.

Nello specifico:

1. Il **docente**, in presenza di contenuti riferiti o mostrati da un alunno che suscitano preoccupazione, ha il dovere di attivare le procedure previste, coinvolgendo a seconda dei casi, i docenti del Consiglio di Classe, il Dirigente Scolastico, il Referente al Bullismo e al Cyberbullismo, i genitori e i servizi territoriali competenti.

Come da art.357 del Codice Penale il docente e il personale operante all'interno della scuola riveste infatti la qualifica di Pubblico Ufficiale e tale ruolo non si estingue al termine delle lezioni ma perdura nelle altre attività correlate, come confermato dalla Corte di Cassazione con la sentenza 15367 del 2014.

2. Gli **alunni/e** possono segnalare atti di bullismo o cyberbullismo, sia se sono vittime dirette sia se assistono agli episodi come testimoni, in vari modi:
 - Parlandone direttamente con il Referente per il Bullismo e Cyberbullismo, con il Coordinatore di Classe o con un insegnante di fiducia, il quale formalizzerà, la segnalazione attraverso la Scheda di prima segnalazione allegata al presente documento;
 - In autonomia utilizzando la scatola/box disponibile in uno spazio accessibile e ben visibile della scuola;
 - Scrivendo una mail all'indirizzo dedicato per gli studenti e le studentesse del secondo ciclo:
antibullismo@iis-sacco.edu.it;
 - Utilizzando il servizio dello sportello di ascolto attivo in orari stabiliti e comunicati regolarmente agli studenti e alle famiglie.
3. Le **famiglie**: anche i genitori devono e possono segnalare casi di sospetto o evidenza dei fenomeni 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...).
4. Il **personale ATA**: segnala al Dirigente Scolastico, al Referente Antibullismo o al docente eventuali atti di bullismo che possono verificarsi negli spazi comuni come corridoi, cortili o ingressi. Ricordiamo che la mancata segnalazione da parte di tutto il personale scolastico costituisce omissione di atto di ufficio come da art. 328 del Codice Penale.

Per tutti coloro, inoltre, che vogliono segnalare una situazione di pericolo e di emergenza in cui sono coinvolti bambini e adolescenti è possibile utilizzare il servizio telefonico «**Emergenza infanzia 114**», attivo su tutto il territorio nazionale, ventiquattro ore su ventiquattro, per tutti i giorni dell'anno. Il **DECRETO LEGISLATIVO 12 giugno 2025, n. 99** recante "Disposizioni in materia di prevenzione e contrasto del bullismo e del cyberbullismo, in attuazione della delega di cui all'articolo 3 della legge 17 maggio 2024, n. 70 ha infatti esteso i servizi offerti dal 114 anche alla prevenzione e al contrasto dei fenomeni del bullismo e del cyberbullismo in tutte le loro manifestazioni, nell'ottica della più ampia tutela delle persone di minore età.

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).

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.
- § **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.
- § **Procura minorile:** segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.
- § **Procure Ordinarie:** nel caso in cui il minore/i sia la vittima/e e il presunto autore del reato sia maggiorenne.

Allegati:

- Scheda di Segnalazione
- Diario di Bordo
- Tabella sanzioni disciplinari contro gli atti di Bullismo e di Cyberbullismo