



Documento di ePolicy

I.C. B. N. SAN C. SUPERSANO

VIA GIACOMO PUCCINI N41 - 73040 - SUPERSANO

Lecce (LE) - Puglia

Data di approvazione: 21/04/2026 - 16:57

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.

Attraverso l'E-Policy il nostro Istituto intende dotarsi di uno strumento operativo di riferimento per tutta la comunità educante, al fine di promuovere un approccio alla tecnologia consapevole, critico ed efficace e di sviluppare, attraverso specifiche azioni, una maggiore conoscenza delle opportunità e dei rischi connessi all'uso di Internet.

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

Di fatto, ragazzi e bambini sono sempre più esposti agli stimoli provenienti dal web, coinvolti in un mondo virtuale nella doppia veste di fruitori e creatori di contenuti. Gli stessi, tuttavia, pur appartenendo alla generazione dei cosiddetti nativi digitali, necessitano di una guida per maturare un approccio responsabile e un atteggiamento vigile che li ponga al riparo dalle insidie. Allo stesso modo, tutta la comunità educante che si relaziona con i nostri studenti si confronta quotidianamente con le TIC e con un sistema comunicativo che si rinnova ogni giorno, diventando più complesso e più ricco, di opportunità, ma anche di pericoli. Per tale motivo, il nostro Istituto ha ravvisato l'esigenza di dotarsi di un documento di E-Policy per fornire il massimo contributo nel percorso di acquisizione di una piena cittadinanza digitale da parte di studenti, studentesse e figure educative, appartenenti al mondo della Scuola o della società civile in generale.

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 segue 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.

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 studenti e le studentesse.

È obbligatorio rispettare la privacy di tutte le persone e, in modo particolare, quella dei minorenni. Ciò riguarda la diffusione e la condivisione di fotografie, immagini, video, ma anche la divulgazione di dati personali. Ogni utilizzo o diffusione di tali informazioni deve avvenire nel pieno rispetto delle norme sulla tutela della privacy e con la massima attenzione alla protezione dei minori.

L'obiettivo del documento di E-Policy consiste nell'individuare regole e comportamenti da condividere con soggetti esterni e per questo è necessario rilevare, prevenire e limitare pericoli legati a condotte educative non professionali. L'Istituto, mediante un'informativa sintetica, chiarisce il sistema di azioni e le procedure di segnalazione, valido anche per professionisti e organizzazioni esterne che entrino in relazione con gli studenti e con la comunità educante. Tale informativa è strettamente necessaria nell'ottica di un miglioramento dei rapporti tra Scuola, famiglie e territorio, permettendo di tutelare gli alunni da comportamenti potenzialmente rischiosi messi in atto da soggetti esterni che si trovano ad operare

all'interno dell'Istituto.

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.

L'E-Policy si integra pienamente con gli obiettivi ed i contenuti dei seguenti documenti del nostro Istituto:

- Piano Triennale Offerta Formativa
- Regolamento di Istituto
- Informativa Privacy
- Codice di comportamento.

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.

Il nostro Istituto condivide e diffonde l'ePolicy agli studenti e alle studentesse, alle famiglie e all'intera comunità scolastica attraverso la pubblicazione del documento sul sito ufficiale della scuola.

La comunicazione avviene inoltre mediante:

- attività di sensibilizzazione sull'uso consapevole e responsabile delle tecnologie digitali;
- la diffusione di una versione *child friendly* del documento, appositamente semplificata per favorire la comprensione e la consapevolezza di bambini/e e ragazzi/e.

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 Team Antibullismo dell'Istituto è promotore di iniziative di sensibilizzazione sul tema dell'importanza della collaborazione tra pari e di una comunicazione non ostile rivolte a studenti, studentesse e famiglie, con l'obiettivo di promuovere un uso delle tecnologie digitali positivo, critico e consapevole, prevenire fenomeni quali il bullismo ed il cyberbullismo e diffondere la cultura della comunicazione non ostile. Promuove, inoltre, momenti di formazione e aggiornamento per il personale scolastico, per la diffusione delle politiche antibullismo adottate dall'Istituto tra le risorse interne al sistema scolastico.

Il gruppo di lavoro che si è occupato della redazione del documento di E-Policy si impegna a monitorare l'efficacia del presente documento, da aggiornare eventualmente in occasione del rinnovo del Piano Triennale dell'Offerta Formativa di Istituto.

Il monitoraggio è necessario per garantire che il documento di e-Policy non resti solo formale, ma sia realmente efficace e aggiornato rispetto ai bisogni della scuola. In particolare perché ciò permette di verificare l'efficacia delle azioni di prevenzione e sensibilizzazione; consente di adattare il documento al contesto scolastico; rende possibile l'individuazione di criticità e la rilevazione di eventuali situazioni di rischio (bullismo, cyberbullismo, uso scorretto della rete). In questo modo l'e-Policy diventa uno strumento utile e concreto per la tutela e la crescita degli studenti.

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](#)

Il nostro Istituto provvede periodicamente all'aggiornamento delle proprie pratiche educative e organizzative, avvalendosi delle risorse, dei materiali formativi e degli strumenti messi a disposizione dal progetto *Generazioni Connesse*, al fine di promuovere un utilizzo sicuro, consapevole e responsabile delle tecnologie digitali.

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.

Nella consapevolezza dell'importanza per le nuove generazioni di sviluppare solide competenze digitali e, al tempo stesso, una piena consapevolezza delle opportunità e delle criticità legate all'uso delle nuove tecnologie, anche il Team per la prevenzione dei fenomeni di bullismo e cyberbullismo, in sinergia con il Team Digitale, ha programmato una serie di interventi educativi e formativi.

Tra questi rientrano, ad esempio, incontri con la Polizia Postale, realizzati in collaborazione con la Prefettura di Lecce, e attività di sensibilizzazione rivolte alle classi, organizzate in occasione della Giornata nazionale contro il bullismo e il cyberbullismo.

Tali iniziative sono finalizzate a promuovere un uso responsabile, sicuro e consapevole della rete, nonché a fornire a studenti e studentesse strumenti concreti per riconoscere, prevenire e contrastare i fenomeni di bullismo e cyberbullismo.

Al fine di favorire un uso consapevole, positivo e produttivo delle TIC, è quanto mai indispensabile la collaborazione dell'intera comunità educante. Scuola e famiglia devono rinforzare l'alleanza educativa e promuovere percorsi formativi continuativi e condivisi per accompagnare insieme bambini/e e ragazzi/e verso un uso responsabile e vantaggioso delle tecnologie digitali. L'Istituto, attraverso azioni mirate, informa le famiglie su tutte le attività e iniziative intraprese sul tema delle tecnologie digitali, previste dall'ePolicy e dal suo Piano di Azioni, aggiornando, al bisogno, il Regolamento d'Istituto e il Patto di corresponsabilità, di cui è parte integrante. In questo modo i genitori saranno costantemente informati sui comportamenti che i propri figli dovranno adottare a scuola e, in generale, riceveranno consigli da mettere in pratica.

A tale scopo saranno previsti incontri di formazione e di sensibilizzazione fra insegnanti e genitori sui temi in oggetto, si individueranno delle modalità per una diffusione capillare del materiale informativo sulle tematiche trattate, messo a disposizione dai siti specializzati (www.generazioniconnesse.it) e dalle forze dell'ordine.

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.

I docenti dei tre ordini di scuola dell'Istituto Comprensivo di Botrugno, Nociglia, San Cassiano e Supersano hanno elaborato un curriculum verticale di Educazione Civica, in linea con la legge 92 del 20 agosto 2019 e con le Linee guida pubblicate con il DM n.35/2020. Tali documenti hanno introdotto l'insegnamento trasversale dell'educazione civica nel primo e secondo ciclo d'istruzione, con iniziative di sensibilizzazione alla cittadinanza responsabile, a partire dalla scuola dell'infanzia e hanno declinato la Competenza digitale secondo le Raccomandazioni del Consiglio Europeo 2006 e successiva revisione 2018. Pertanto, i consigli dei tre ordini di scuola dell'Istituto, per mezzo di percorsi di apprendimento singolo e/o multidisciplinare, programmati collegialmente e monitorati costantemente in fase di attuazione, come pure di iniziative di sensibilizzazione alla cittadinanza responsabile, anche in collaborazione con gli Enti locali, hanno promosso lo sviluppo delle competenze civiche e sociali da parte degli studenti.

L'animatore Digitale e il Team hanno elaborato un Curriculum Digitale per l'Istituto nel rispetto delle Competenze Chiave Europee del 2018 e del Quadro comune di riferimento europeo per le competenze digitali Modello Europeo DigComp 2.2. Difatti, l'Istituto, impegnato nell'implementazione e sperimentazione del curriculum verticale per le competenze digitali, partecipa al progetto Safer Internet Centre - Generazioni Connesse: <https://www.generazioniconnesse.it/site/it/safer-internet-centre/> e ha attivato percorsi per lo sviluppo delle competenze STEM come previsto dal DM n.65/2023 (ad esempio: Formazione PEKIT, Percorsi di orientamento e formazione per il potenziamento delle competenze STEM, digitali e di innovazione).

2.3 - Il Kit Didattico

L'e-Policy 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 Didattico di Generazioni Connesse sarà utilizzato dai docenti del Team antibullismo e cyberbullismo dell'Istituto, insieme ai materiali educativi messi a disposizione dalla piattaforma Parole O_Stili, per realizzare attività di informazione, formazione e sensibilizzazione rivolte agli studenti.

Tali strumenti didattici consentiranno di affrontare in modo strutturato i temi del rispetto online, dell'uso consapevole della rete e della prevenzione dei fenomeni di bullismo e cyberbullismo, favorendo lo sviluppo di comportamenti responsabili e di una cittadinanza digitale attiva.

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.

La scuola non ha solo il compito di tutelare la privacy degli studenti, delle studentesse e delle loro famiglie, ma anche quello di rendere consapevoli gli utenti di quanto sia importante tutelare il diritto alla riservatezza di se stessi e degli altri. La diffusione sempre maggiore di smartphone tra i giovanissimi, la condivisione online di contenuti didattici, l'uso del registro elettronico Nuvola e di piattaforme per la Didattica Digitale Integrata, come Microsoft Teams, obbliga la scuola ad avere un'attenzione particolare non solo alla privacy in generale, ma anche alla gestione della privacy legata all'uso dei nuovi dispositivi.

L'Istituzione scolastica ha facoltà di trattare solo i dati personali necessari al perseguimento di specifiche finalità istituzionali, oppure quelli espressamente previsti dalla normativa di settore. In questi casi non è tenuta a chiedere il consenso al trattamento dei dati personali. Al contrario, dati sensibili e giudiziari devono essere trattati nel rispetto di specifiche norme di legge, verificandone la pertinenza e la completezza, ma anche la loro indispensabilità rispetto alle "finalità di rilevante interesse pubblico" che si intendono perseguire. La scuola ha, inoltre, l'obbligo di informare gli interessati delle caratteristiche e delle modalità del trattamento dei loro dati, indicando i responsabili dello stesso. Gli interessati di tale informativa non sono solo studenti e studentesse, ma anche le famiglie, i docenti e la comunità educante tutta.

Lo strumento ufficiale e principale che l'Istituto utilizza per comunicare e condividere informazioni e iniziative all'esterno è il sito web istituzionale della scuola, ovvero, <https://icbnscs.edu.it/>. Per la comunicazione interna l'Istituto fa riferimento al Registro Elettronico Nuvola, con tutte le sue funzionalità, e alla piattaforma Microsoft Teams, di cui ci si avvale per la condivisione di materiali didattici con gli studenti e per la predisposizione di ambienti virtuali di lavoro tra docenti, nonché per l'organizzazione di incontri istituzionali online.

Il Registro elettronico è anche lo strumento che funge da "ponte" tra scuola e famiglie. Queste ultime, infatti, mediante semplici clic, possono monitorare il percorso didattico-educativo dei propri figli. Gli insegnanti aggiornano quotidianamente il registro, riportando le assenze, dettagliando argomenti e attività svolti in classe, compiti per casa, valutazioni, informazioni

sull'andamento didattico-disciplinare degli alunni, comunicazioni rivolte alle famiglie. Tramite il registro i docenti possono anche condividere circolari destinate ad una specifica classe.

La piattaforma Microsoft Teams rappresenta un'altra risorsa preziosa perché, permettendo la comunicazione e la condivisione di materiale didattico, favorisce lo sviluppo delle competenze digitali degli studenti che si avvicinano alla gestione attiva dello stesso e, al contempo, garantisce la dematerializzazione, altro aspetto positivo assicurato dalle TIC.

Per quanto riguarda la comunicazione interna, il nostro Istituto persegue l'obiettivo di garantire il "diritto alla disconnessione". L'art. 22 (Livelli, soggetti, materie di relazioni sindacali per la Sezione Scuola) del CCNL 2016/2018, infatti, fa riferimento ai criteri generali per l'utilizzo di strumentazioni tecnologiche di lavoro in orario diverso da quello di servizio, al fine di una maggiore conciliazione fra vita lavorativa e vita familiare.

Le azioni intraprese e le eventuali violazioni della sicurezza, nonché le informazioni sul corretto/ scorretto utilizzo dei dispositivi (personali e non) sono esplicitate sul sito d'Istituto nelle sezioni Privacy Policy e Regolamento d'Istituto.

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 - 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.

Il nostro Istituto considera le TIC una risorsa da integrare nella didattica, anche e soprattutto per potenziare l'inclusività e la personalizzazione delle diverse proposte in base agli stili cognitivi e di apprendimento degli studenti.

Secondo quanto previsto dalla Legge 107 del 2015, "al fine di sviluppare e di migliorare le competenze digitali degli studenti

e di rendere la tecnologia digitale uno strumento didattico di costruzione delle competenze in generale, il Ministero dell'istruzione, dell'Università e della Ricerca adotta il Piano nazionale per la scuola digitale (...)” e “la scuola digitale, in collaborazione con le famiglie e gli enti locali, deve aprirsi al cosiddetto BYOD (Bring Your Own Device), ossia a politiche per cui l'utilizzo di dispositivi elettronici personali durante le attività didattiche sia possibile ed efficace”.

BYOD è un'espressione che letteralmente significa “porta il tuo dispositivo”; sulla base di tale concezione i tablet e i pc possono essere integrati nel lavoro nelle classi in base ad obiettivi formativi e didattici programmati. Nel nostro Istituto alcuni docenti hanno integrato la modalità BYOD nella didattica quotidiana, previa autorizzazione scritta rilasciata dalle famiglie. Gli insegnanti che propongono attività BYOD pianificano la lezione sotto la propria responsabilità, assumendosi l'onere del controllo e della supervisione dell'utilizzo dei dispositivi da parte degli alunni. Durante alcune lezioni, dunque, gli alunni possono utilizzare tablet e PC per svolgere attività didattiche di vario tipo, come test, esercitazioni interattive, Kahoot ecc. Tali proposte consentono ai docenti stessi di rendere gli studenti più “esperti” nell'utilizzo delle TIC, mediante condivisione di suggerimenti e indicazioni per un utilizzo creativo, ma anche critico e consapevole delle stesse.

Il possesso di tali dispositivi a scuola è disciplinato dagli artt. 8 e 9 del nostro Regolamento d'Istituto che, recependo la Circolare Ministeriale n.5274 dell'11 Luglio 2024 sulle Disposizioni in merito all'uso degli smartphone e del registro elettronico nel primo ciclo di istruzione, la quale prevede “...il divieto di utilizzo in classe del telefono cellulare, anche a fini educativi e didattici, per gli alunni della scuola dell'infanzia fino alla secondaria di primo grado, salvo i casi in cui lo stesso sia previsto dal Piano educativo individualizzato o dal Piano didattico personalizzato, come supporto rispettivamente agli alunni con disabilità o con disturbi specifici di apprendimento ovvero per documentate e oggettive condizioni personali. Potranno, invece, essere utilizzati, per fini didattici, altri dispositivi digitali, quali pc e tablet, sotto la guida dei docenti. Restano fermi, dunque, il ricorso alla didattica digitale e la sua valorizzazione...”.

Infatti, in ottemperanza dell'art. 5, comma 2, della Legge 20 agosto 2019, n. 92 (cittadinanza digitale) che prevede che l'offerta formativa dell'insegnamento dell'educazione civica includa competenze digitali essenziali, sviluppate gradualmente in base all'età, e coerentemente con le Raccomandazioni del Consiglio Europeo 2006 e la successiva revisione 2018, nelle quali la Competenza digitale, considerata una delle otto competenze chiave per l'educazione permanente, è definita come la capacità di utilizzare con dimestichezza e spirito critico le tecnologie della società dell'informazione, il nostro Istituto ha redatto un Curricolo Digitale verticale che ha come Quadro di riferimento per le competenze digitali il Modello Europeo DigComp 2.1.

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.

Il nostro Istituto adotta azioni di sensibilizzazione e prevenzione, mirate a:

-informare e formare docenti, personale ATA e allievi sui rischi di un utilizzo non sicuro degli strumenti digitali per la didattica e l'apprendimento con l'ausilio del Team per l'Innovazione Digitale;

-favorire il coinvolgimento dei genitori nel percorso dei propri figli e nelle attività di formazione legate ad un uso corretto delle tecnologie digitali;

-avvalersi della figura del Referente per il contrasto ai fenomeni di bullismo e cyberbullismo e dell'intero Team Antibullismo e per l'Emergenza con il compito di definire, coordinare e monitorare iniziative di prevenzione e sensibilizzazione.

Il nostro Istituto promuove una didattica inclusiva volta alla valorizzazione di ogni diversità. Attraverso il curriculum trasversale di Educazione Civica, integrato all'interno del PTOF, si attuano percorsi di riflessione sull'alterità, l'accoglienza e la multiculturalità come parte integrante dell'attività didattica.

La comunità scolastica è consapevole di dover segnalare tutti i casi di bullismo, cyberbullismo, adescamento online, uso poco sicuro di internet e dei social network, sexting, e qualsiasi altro fenomeno che provochi situazioni di disagio, a carico di qualsiasi soggetto appartenente alla comunità stessa, o che costituisca reato.

Per favorire un uso consapevole delle tecnologie digitali vengono svolte attività di riflessione e metacognizione sulle abitudini digitali degli alunni. Laddove emergano segnali di disagio legati a fenomeni di iperconnessione o all'uso compulsivo dei dispositivi, la scuola, attraverso le proprie figure di riferimento, provvederà a coinvolgere attivamente le famiglie per strutturare percorsi di supporto con il contributo del Team per l'Innovazione Digitale.

In presenza di rischi per il benessere psicofisico dei minori l'Istituto si impegna all'attivazione di percorsi di supporto psicologico. A tal fine, collabora con i servizi socio-sanitari presenti sul territorio (Consultori familiari, Servizi di Neuropsichiatria infantile, centri specializzati sull'abuso e il maltrattamento dell'infanzia, etc.) e le Autorità competenti (Prefettura, Polizia di Stato e Arma dei Carabinieri).

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

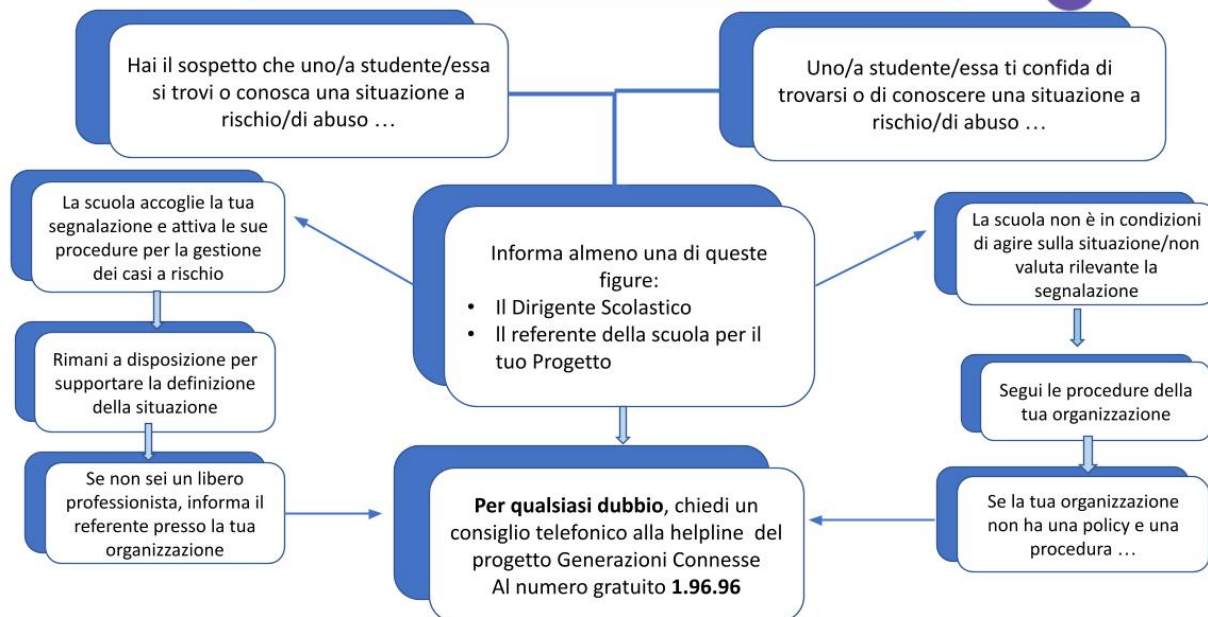
Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione: un indirizzo e-mail specifico per le segnalazioni; scatola/box per la raccolta 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.

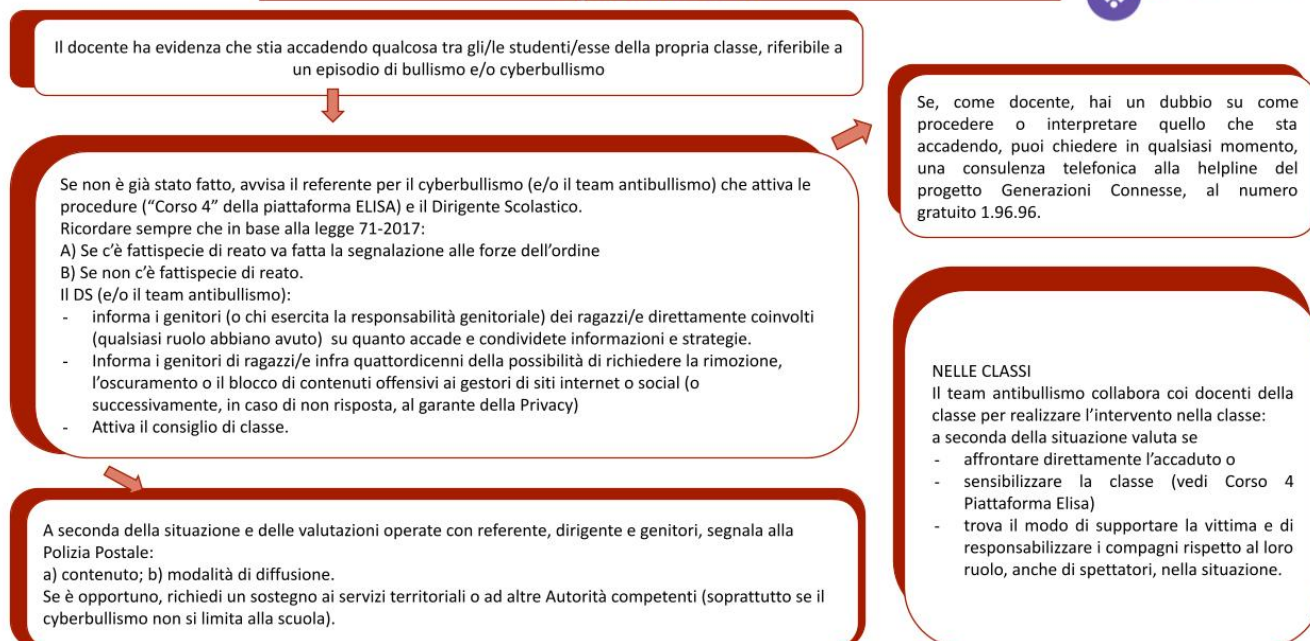
Per ulteriori chiarimenti in merito, si rimanda al Regolamento di disciplina degli studenti e delle studentesse, integrato con la previsione di infrazioni disciplinari legate a comportamenti scorretti assunti durante la DID e relative sanzioni, alle [Linee di Orientamento per la prevenzione e il contrasto 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 di segnalazione per enti, associazioni, professionisti esterni alla scuola



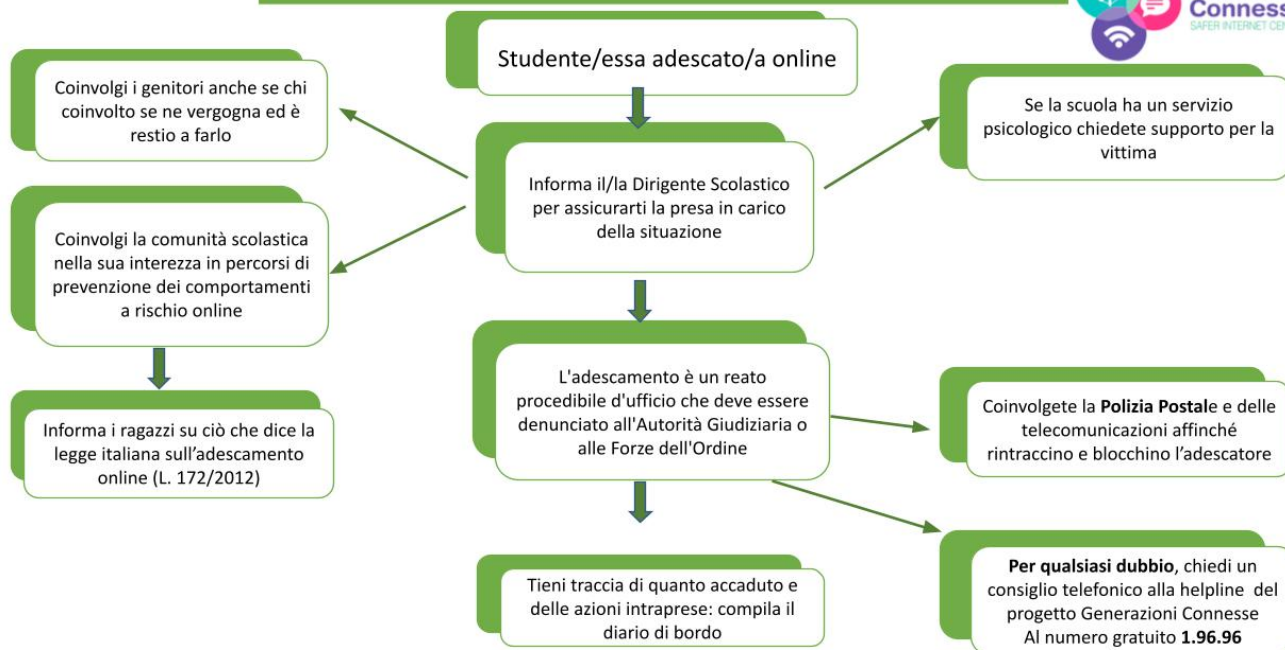
Procedure interne: cosa fare in caso di evidenza di Cyberbullismo

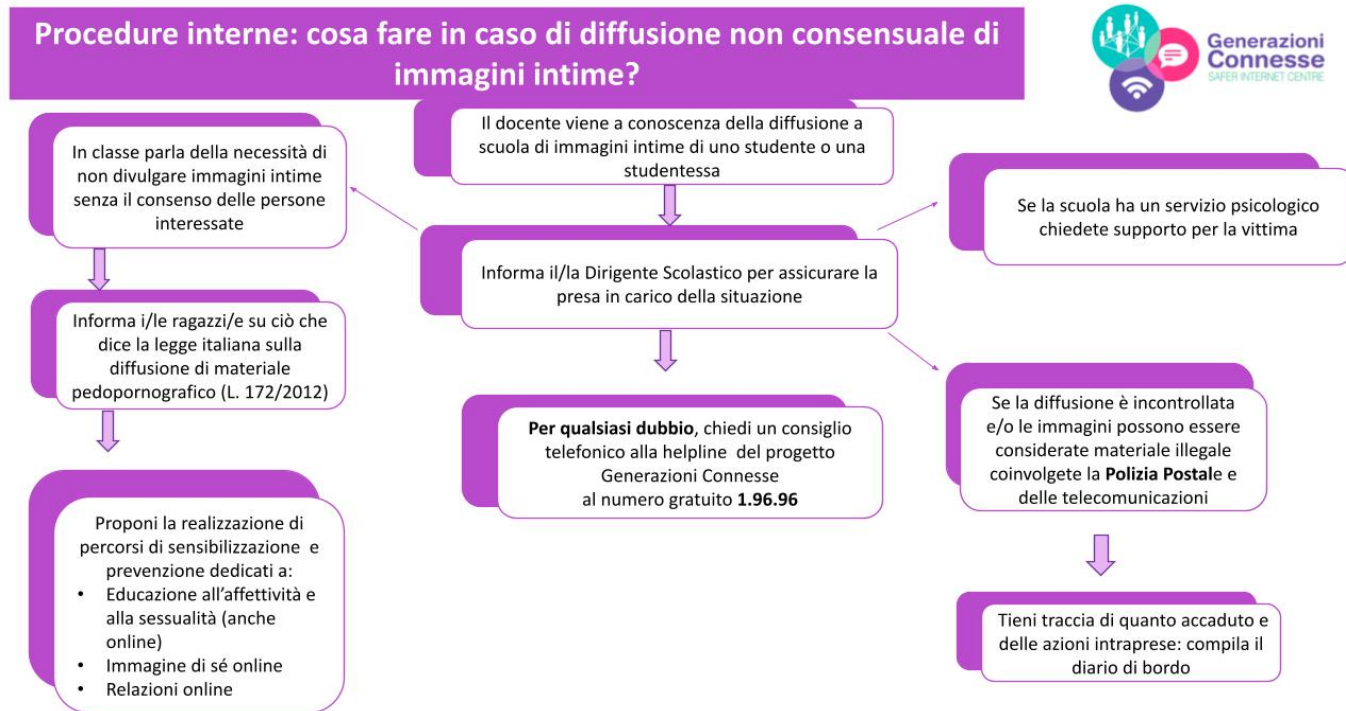


Procedure interne: cosa fare in caso di sospetto di Cyberbullismo



Procedure interne: cosa fare in caso di Adescamento Online?





Il nostro Istituto ha elaborato un Codice Interno per la prevenzione ed il contrasto di fenomeni di bullismo e cyberbullismo che rappresenta il punto di riferimento non soltanto di tutta la comunità scolastica, ma anche degli attori esterni che dovessero entrare ad operare nel contesto Scuola.

Le situazioni di emergenza sono gestite e monitorate dal docente Referente per il contrasto al bullismo e al cyberbullismo insieme al Team Antibullismo e al Team per l' Emergenza.

La squadra di Istituto potrà avvalersi anche del contributo del personale non docente (es. collaboratori scolastici) e di altre figure professionali (es. psicopedagogisti), queste ultime in base a quanto previsto dalle risorse a disposizione.

Il team Anti Bullismo e il Team per l'Emergenza si occupano:

- della presa in carico della prima segnalazione;
- della valutazione approfondita (livello di gravità e relativi interventi);
- di monitorare il caso nel tempo;
- di proporre e organizzare interventi formativi e rieducativi;
- di lavorare in sinergia con i servizi presenti sul territorio, in caso di necessità.

Il team agisce prevalentemente durante l'orario scolastico ed entro tempi brevi dalla prima segnalazione del caso in

questione.

Il protocollo di riferimento per la gestione dei casi, contenuto nel Codice Interno per la prevenzione ed il contrasto di fenomeni di bullismo e cyberbullismo, prevede 4 fasi:

1^ FASE: PRIMA SEGNALAZIONE

Il caso potrà essere segnalato da genitori, alunni, insegnanti, collaboratori scolastici o soggetti esterni che si trovano ad operare a Scuola. La prima segnalazione attiva un percorso di osservazione, di analisi e di valutazione di un presunto caso di bullismo, cyberbullismo, abuso o disagio legato ad un uso scorretto delle TIC.

2^ FASE: LA VALUTAZIONE APPROFONDITA

La valutazione approfondita viene condotta dal Team con il supporto dei docenti della squadra per le Emergenze e con la collaborazione dei docenti del Consiglio della classe coinvolta. Tale fase riguarda l'individuazione della tipologia e della gravità del caso attraverso:

- la raccolta di informazioni sull'accaduto e la ricostruzione della dinamica dei fatti;
- la valutazione della tipologia del/degli episodi;
- la raccolta di informazioni sui soggetti coinvolti nei diversi ruoli (attori, vittime, testimoni);
- la comprensione del livello di disagio della vittima;
- la valutazione delle caratteristiche di rischio del bullo.

3^ FASE: GESTIONE DEL CASO E SCELTA DELLA TIPOLOGIA D'INTERVENTO

In base all'analisi compiuta si delinea il livello di priorità dell'intervento, che può essere meno grave (verde), più grave (giallo) o di significativa gravità (rosso).

Gli interventi previsti sono:

- Approccio educativo destinato all'intera classe: condotto dagli insegnanti della classe con l'ausilio del Team per l'emergenza nella fase progettuale. L'obiettivo principale è quello di sensibilizzare e responsabilizzare la classe.
- Intervento individuale, caratterizzato da: un colloquio di supporto con la vittima; un colloquio "riparativo" con il bullo, condotto da insegnanti dotati di competenze e formazione adeguata sul tema e alla presenza di un membro del Team o di un insegnante di classe; l'attuazione di eventuali misure sanzionatorie - previste nel Regolamento d'Istituto - da parte del Consiglio di Classe, che a tal fine adotterà il procedimento disciplinare previsto; interventi psico-educativi operati da specialisti.
- Coinvolgimento della famiglia: come specificato nell'art.5 della Legge 71/2017 "Salvo il fatto costituisca reato, il Dirigente Scolastico che venga a conoscenza di atti di cyberbullismo informa tempestivamente i soggetti esercenti la responsabilità genitoriale ovvero i tutori dei minori coinvolti e attiva adeguatamente azioni di carattere educativo." L'intervento sarà condotto dal Dirigente Scolastico ed eventualmente dal Referente o altro membro del Team allo scopo di rendere la famiglia parte attiva nella risoluzione del problema.

- Supporto intensivo a lungo termine e di rete: consiste nell'attivazione da parte della scuola, nella figura del Dirigente Scolastico, di un ponte famiglia - istituzioni territoriali. Il Team per l'emergenza, una volta decisa la tipologia di intervento da attuare, ha il compito di coinvolgere le altre figure che interverranno nella realizzazione dell'intervento/degli interventi.

4^ FASE: IL MONITORAGGIO

Il monitoraggio permette di capire se i correttivi apportati sono risultati adeguati o se sono necessarie azioni aggiuntive.

Il presente Codice e la relativa modulistica, opportunamente adattati, sono stati elaborati facendo riferimento al materiale messo a disposizione sulla Piattaforma ELISA (progetto di formazione e-learning nato dalla collaborazione tra MIUR - Direzione generale per lo studente e il Dipartimento di Formazione, Lingue, Intercultura, Letterature e Psicologia dell'Università di Firenze).

Il Codice interno per la prevenzione ed il contrasto di fenomeni di bullismo e cyberbullismo costituisce parte integrante:

- del Regolamento d'Istituto;
- del Piano Triennale dell'Offerta Formativa;
- del Patto di Corresponsabilità Educativa.