Istituto Istruzione Superiore "E. Fermi – Guttuso"
95014 - Giarre (CT)
OSSERVATORIO D'AREA DISPERSIONE N.8
Sede Amministrativa: Via N. Maccarrone, 4 – Tel. 095-6136555
PEC ctis03900q@pec.istruzione.it **e-mail** ctis03900q@istruzione.it
http://www.isfermiguttuso.edu.it
Codice Fiscale 92030810870
Codice Univoco Fatturazione Elettronica UF2MKU

IIS - "E. FERMI - GUTTUSO"-GIARRE
Prot. 0002967 del 11/02/2025
V (Uscita)

Approvato con deliberazione del Consiglio di Istituto in data 10/02/2025

Regolamento di ePolicy per il contrasto al bullismo e cyberbullismo

Capitolo 1 - Presentazione dell'ePolicy

1. Scopo dell'ePolicy
2. Ruoli e responsabilità nell'implementazione dell'ePolicy
3. Integrazione ePolicy nei documenti scolastici
4. Condivisione e comunicazione dell'ePolicy all'intera comunità educante
5. I piani di Azione dell'ePolicy
6. Le risorse di Generazioni Connesse

Capitolo 2 - Sensibilizzazione e prevenzione

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:

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

Attraverso l'ePolicy, si intende promuovere:

L'uso consapevole, critico e sicuro delle tecnologie digitali e di Internet, incoraggiando gli studenti a sviluppare competenze tecniche e comportamentali per una corretta cittadinanza digitale.

La prevenzione e la gestione delle problematiche connesse a un utilizzo non responsabile, pericoloso o dannoso delle tecnologie, compresa l'esposizione a rischi quali contatti con contenuti inadeguati o illegali, cyberbullismo, violazioni della privacy e altri comportamenti illeciti.

La collaborazione tra scuola e famiglie per educare studenti e comunità scolastica a un utilizzo etico e responsabile delle tecnologie, sia a scuola sia nella vita quotidiana.

Gli utenti, in particolare i minori, devono essere pienamente consapevoli dei rischi derivanti dalla navigazione in rete. Per ridurre tali rischi, l'Istituto adotta strategie educative e preventive, promuovendo anche il dialogo con enti esterni come Polizia Postale o altre autorità competenti per affrontare situazioni di particolare gravità.

Responsabilità condivisa

L'intera comunità scolastica – insegnanti, personale ATA e famiglie – ha un ruolo attivo nell'educare gli studenti al rispetto delle norme, dei diritti e della privacy, contribuendo a prevenire situazioni di rischio e a diffondere un approccio consapevole alla tecnologia.

Monitoraggio e aggiornamento/rinnovo

La ePolicy ha validità triennale, ma prevede un monitoraggio annuale per verificare la sua efficacia e attualità rispetto all'evoluzione delle tecnologie digitali e delle normative. Gli obiettivi del monitoraggio sono:

- ✓ valutare la situazione iniziale e finale delle classi in relazione all'uso sicuro e responsabile delle tecnologie digitali
- ✓ identificare le necessità formative degli studenti, del personale scolastico e delle famiglie
- ✓ analizzare eventuali incidenti o criticità emerse per migliorare le strategie educative e preventive

Il monitoraggio e l'aggiornamento della ePolicy sono curati dal Dirigente Scolastico, con il supporto di Commissioni create ad hoc. Al fine di garantire una prospettiva inclusiva e partecipata la partecipazione sarà estesa a rappresentanti del personale ATA, degli studenti e delle famiglie.

Approvazione e trasparenza
Le eventuali modifiche della ePolicy saranno discusse e approvate nel Collegio dei Docenti e nel Consiglio d'Istituto.

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

I REFERENTI PER IL BULLISMO E CYBERBULLISMO

I referenti cyberbullismo è co-responsabile, con il team ePolicy, dell'attuazione dei piani di azione e coordina le iniziative di prevenzione e contrasto del c y b e r b u l l i s m o .

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 pedagogista, se presente) nelle situazioni acute di bullismo.
Promuovere la redazione e l'applicazione della ePolicy e monitorare le segnalazioni.

Psicologo

Supporta il team Antibullismo e per l'Emergenza nella gestione dei casi segnalati.
Accoglie segnalazioni da studenti, famiglie, docenti e personale ATA, fornendo supporto relazionale.

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 meritoagli obblighi derivanti dal GDPR e sorveglia sull'esatta osservanza della normativa in materia di tutela dei dati personali ed èco-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/sse 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.

Corresponsabilità educativa e formativa

Nel percorso di crescita degli studenti e delle studentesse, esiste una corresponsabilità educativa e formativa che coinvolge genitori e scuola. Dal punto di vista giuridico, questa responsabilità è declinata in tre tipologie di "culpa" applicabili anche ai problemi derivanti dall'uso improprio delle tecnologie digitali:

Culpa in vigilando (art. 2048, comma 2 c.c.): riguarda la mancata sorveglianza attiva del docente responsabile nei confronti del minore. Tale responsabilità è superabile attraverso una prova liberatoria che dimostri l'impossibilità di impedire il fatto (art. 2048, comma 3 c.c.).

Culpa in organizzando: si riferisce alla mancata adozione di provvedimenti adeguati da parte del Dirigente Scolastico per prevenire eventuali incidenti.

Culpa in educando (art. 30 Costituzione, art. 2048, comma 1 c.c., art. 147 c.c.): riguarda i genitori, che hanno il dovere di instaurare una relazione educativa adeguata, volta a prevenire comportamenti dannosi verso terzi.

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 MIM 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.

1.4 Condivisione e comunicazione dell'ePolicy

Il paragrafo dettaglia i seguenti aspetti:

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

***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.

L'ePolicy è un documento articolato, composto da norme, indicazioni, linee guida, metodologie e approfondimenti. Per garantire un'efficace comunicazione, è essenziale adattare contenuto e linguaggio in funzione dei diversi destinatari.

Pertanto, il nostro Istituto predisporrà versioni ridotte e mirate del documento per ciascun target e attiverà un percorso di informazione e formazione adeguato per la comunità scolastica. La seguente tabella esplicita i destinatari, i contenuti e le modalità di comunicazione:

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.

Monitoraggio e Valutazione del processo di ePolicy

Il monitoraggio e la valutazione del processo di ePolicy rappresentano elementi chiave per garantire l'efficacia delle azioni intraprese e il miglioramento continuo. Queste attività sono condotte dalla Commissione Monitoraggio e Valutazione ePolicy e si svolgono parallelamente all'implementazione, fornendo feedback costanti alla Commissione ePolicy. Questo approccio permette di ottimizzare le strategie e di rispondere in maniera dinamica alle esigenze emergenti.

Fin dalle prime fasi la Commissione dovrà identificare indicatori chiave, strumenti di raccolta dati e benchmark di riferimento definendo così un sistema di valutazione capace di misurare i benefici generati dall'ePolicy per i seguenti gruppi:

Studenti, con particolare attenzione alla crescita delle competenze digitali, al benessere e alla sicurezza online.

Personale scolastico, valutando il livello di formazione, consapevolezza e capacità di gestire le tematiche legate all'ePolicy.

Famiglie, misurando il grado di coinvolgimento e l'impatto delle attività formative.

Comunità allargata, includendo eventuali partner, enti locali o realtà sociali coinvolte (ad es. evento informativo o formazione rivolti al territorio).

Il processo di valutazione sarà condotto annualmente e la valutazione al termine del percorso triennale costituirà ilpunto di partenza per l'aggiornamento del prossimo documento.

Nota: per le rilevazioni si potranno utilizzare SELFIE https://education.ec.europa.eu/it/selfie predisposto dalla Commissione europea e/o MyDigSkills https://mydigiskills.eu/it/

1.6 - Le risorse di Generazioni Connesse

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.

Per lo sviluppo di attività didattiche e per la formazione della comunità scolastica 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 differenti)
Canale TikTok
Canale Instagram
Canale Facebook

Cap 2 - Sensibilizzazione e prevenzione

La quotidianità in rete di ciascuno dei componenti della comunità scolastica - docenti, studenti e famiglie - deve essere caratterizzata da una consapevolezza critica delle caratteristiche degli ambienti e dei servizi online affiancata alle competenze per vivere al meglio il mondo connesso.

In questa direzione l'ePolicy è un documento che sviluppa azioni e interventi con l'obiettivo di raggiungere l'intera comunità scolastica e promuovere, ciascuno secondo il proprio ruolo, una cittadinanza digitale composta dalla conoscenza dei diritti in rete, dei rischi e delle opportunità per una partecipazione attiva e responsabile nella rete.

L'Istituto condivide il principio che la prevenzione parta dalla conoscenza e quindi si impegna a portare avanti percorsi volti a educare la Comunità scolastica all'uso consapevole e responsabile delle tecnologie digitali. Questo avverrà attraverso la formazione e l'implementazione di un curricolo digitale che parta dal DigComp 2.2 e il coinvolgimento delle Famiglie.

Nel prossimo triennio, sarà fondamentale rendere la competenza digitale una componente strutturale di tutti i percorsi formativi, integrandola anche attraverso l'insegnamento dell'Educazione Civica, che è trasversale a tutte le discipline.

Il Progetto di Educazione Civica 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.

Il progetto mira inoltre a educare i ragazzi 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.

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 curricolo di educazione alla Cittadinanza Digitale previsto dalla L. 92/2019. Il curricolo prende forma attorno all'ePolicy e le attività didattiche sono legate al documento ed alle scelte dell'Istituto al suo interno.

Nel curricolo 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 Curricolo Digitale si basa sul Framework Europeo DigComp 2.2, che identifica le competenze digitali fondamentali per cittadini e professionisti del XXI secolo. L'approccio adotta una visione sistemica, declinando le 5 aree di competenza del framework per rispondere alle esigenze specifiche degli studenti e del contesto educativo tecnico-industriale.

Obiettivi Generali

- Promuovere competenze digitali strutturate: allineare l'istruzione digitale alle 5 aree di competenza del DigComp 2.2.
- Rendere gli studenti cittadini digitali consapevoli: formare competenze per un utilizzo etico e responsabile delle tecnologie.
- Sviluppare abilità tecniche avanzate: integrare competenze specifiche per il settore industriale e tecnologico.
- Incoraggiare un apprendimento continuo e autonomo: preparare gli studenti a sviluppare competenze digitali lungo tutto l'arco della vita.

Il Curricolo Digitale si basa su:

- Didattica laboratoriale: approccio pratico in laboratori informatici e tecnologici.
- Interdisciplinarità: integrazione delle competenze digitali con altre discipline di indirizzo.
- Problem-based learning: attività che stimolano il pensiero critico e la risoluzione di problemi reali.

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 diun 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 gestione della privacy ottempera pienamente alle indicazioni del GDPR 679/2016 del D.lsgs 196/2003.

E' stato pubblicato sul sito d'Istituto il "REGOLAMENTO PER L'UTILIZZO DI INTERNET, DELLE APPARECCHIATURE E DEI LABORATORI INFORMATICI" che definisce il protocollo per il trattamento dei dati sensibili informatizzati
Link sito internet

è stata pubblicata sul sito d'Istituto l'informativa relativa al trattamento dei dati personali degli utenti che visitano il portale dell'Istituto Link sito internet

In particolare preme evidenziare quanto sotto riportato.

Dati Sensibili degli Studenti:

Se cartacei, sono custoditi in armadi metallici dotati di serratura che viene chiusa quando l'ufficio è chiuso al pubblico. Gli unici operatori atti a poter accedere alle informazioni sensibili sono rappresentati dal personale amministrativo in forza all'ufficio, dai docenti referenti per il sostegno in Istituto e dai docenti Coordinatori di Classe.
Tutto il personale docente e non docente ha sottoscritto l'accettazione delle norme in materia di Privacy dei dati ed ha seguito un corso erogato dal DPO (Data Protection Officer) dell'Istituto. Non vengono mai trasmessi dati sensibili via email; le famiglie degli studenti per i quali occorre redigere apposita documentazione sono convocate fisicamente a scuola, rispettando le rigorose disposizioni in materia di sicurezza sanitaria, per l'apposizione della firma sui relativi documenti, es. PEI, PDP, etc.

Per quanto concerne l'elaborazione e la manutenzione dei dati sensibili in possesso degli uffici memorizzati in modo digitale, queste vengono attuate da specifiche procedure attraverso il browser utilizzando credenziali personali (Username e Password) degli addetti degli uffici. Il sistema di accesso è impostato in maniera tale da obbligare gli utenti al cambio della password di accesso ogni 3 o 6 mesi, secondo il tipo di contenuto memorizzato.

Dati sensibili mantenuti al di fuori degli Uffici Didattici e Amministrativi:

Si specifica che nelle zone dell'istituto ove si erogano attività didattiche come aule, laboratori, aule speciali, non vengono mai mantenuti o trattati documenti che contengano dati sensibili di personale interno, genitori, famiglie o di studenti.

La Privacy nelle Attività Didattiche:

Tutte le attività didattiche fanno uso di piattaforme validate dal Ministero della Pubblica Istruzione, in questo caso viene utilizzato il sistema Google WorkSpace for EDU per la posta elettronica Google Mail, le videoconferenze con Google Meet, le lavagne digitali, le classi virtuali in modalità eLearning con Google Classroom e Google Drive per il mantenimento dei dati. Durante la fase di iscrizione in istituto alle Famiglie (se minorenni) o direttamente agli studenti negli altri casi, viene chiesto di leggere il regolamento interno all'uso delle Google WorkSpace for EDU e di sottoscriverlo tramite firma autografa che viene conservata nel fascicolo personale dello studente. Gli studenti che smarriscono la password di accesso vengono segnalati al Dirigente Scolastico e all'Animatore Digitale come inadempienti alla norma che li obbliga ad effettuare un rigorosa e sicura manutenzione e memorizzazione della password di accesso. Il sistema Google WorkSpace for EDU viene amministrato da un Team di docenti nominati dal Dirigente Scolastico per questo scopo, assegna le password e fornisce agli studenti, durante il primo anno di iscrizione, la formazione necessaria per poter operare in autonomia e sicurezza con tutti gli strumenti digitali.

Tutto il Personale Scolastico è dotato di credenziali di accesso per poter utilizzare, con livelli differenti di autorizzazioni, gli strumenti Google Workspace for EDU (Posta elettronica, Cloud Drive, e-Learning, Videoconferenze per riunioni e lezioni in modalità sincrona).

Il sistema di posta elettronica e di mantenimento file del sistema Google WorkSpace for EDU possiede filtri evoluti per segnalare anomalie nei messaggi ricevuti ed inviati, cosi come per i files memorizzati nel Cloud Google (GDrive).

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.

Tipologia di accesso alla rete Internet:

L'accesso ad Internet all'interno dell'Istituto avviene su distribuzione nei vari ambienti effettuato tramite connessione cablata ethernet a 100-1000Mbps, e tramite connettività Wireless, tramite WLAN Wi-Fi a 2.4-5GHz. L'accesso ad internet è, per gli uffici didattici/amministrativi, separato dall'accesso Didattico, stante l'esistenza di due reti separate fisicamente. La tecnologia usata da parte dei vari provider che forniscono accesso alla scuola è di tipo FTTC (Fiber To The Cabinet) per alcune linee già presenti in istituto da tempo, mentre di tipo FTTH (Fiber To The Home) per le nuove linee fornite direttamente dal consorzio GARR Italiano e dai provider Vodafone e Wind con contratti di tipo Aziendale. All'interno dell'Istituto, essendovi un congruo numero di edifici distribuiti su una ampia superficie, si procede alla distribuzione del segnale tramite dorsale in fibra ottica mono-modale con tratte a 1 e 10Gbps.

Diritti di accesso alla rete:

Uffici:

La connessione alla rete internet da parte del personale amministrativo è possibile utilizzando credenziali di accesso locali. Tutte le connessioni sono filtrate de firewall con servizio di Content Filtering in abbonamento o limitazioni alla navigazione in Internet.

Laboratori Didattici:

La connessione all'interno dei laboratori avviene utilizzando i PC del laboratorio. L'istituto utilizza il servizio Flashstart come firewall per la navigazione sul web, il sistema filtra gli accessi in base al tipo di contenuto dei vari siti web, consentendo la consultazione se appartenenti a categorie idonee. I docenti presenti nei laboratori sono responsabili dell'uso della rete Internet che gli studenti fanno durante le lezioni.

Classi:

La connessione all'interno delle classi alla rete Internet viene effettuata dai soli docenti che utilizzano il Registro Elettronico di Istituto attraverso gli strumenti resi disponibili dalla rete Internet per le attività didattiche. Tali connessioni avvengono tramite PC dell'aula o laptop di proprietà dell'insegnante o fornito dall'Istituto, previo inserimento delle credenziali di accesso controllate da server RADIUS. Tali connessioni subiscono log e filtro dei contenuti acceduti utilizzando il servizio Flashstart; la connessione può avvenire tramite WiFi o con cavo Ethernet. Gli studenti, a meno che non svolgano attività didattiche che richiedano l'uso della rete e dei dispositivi personali in modalità BYOD (Bring You Own Device) non hanno il permesso,

né credenziali apposite per connettersi alla rete in modalità WiFi. L'uso del cellulare durante le attività didattiche che non prevedano espressamente la modalità BYOD è tassativamente vietato attraverso normativa interna e Ministeriale MIUR.

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

Suite Educational in uso:

Come indicato in precedenza a proposito dell'uso della Privacy in Istituto, tutti gli strumenti inerenti alla Didattica sono stati scelti sulla base diaffidabilità, garanzia della privacy, anche seguendo le indicazioni date dal Ministero della Pubblica Istruzione MIUR. A tale scopo sono stati, a partire dall'anno scolastico 2016-17, individuati i sistemi Google Suite for Education, ora nominato Google WorkSpace for Education (EDU) e ilSistema Microsoft Office365 for Education (EDU), entrambi forniti dalle rispettive multinazionali Google e Microsoft a titolo gratuito in uso a Istituti Scolastici.

Strumenti Utilizzati da Docenti e Studenti:

Per quanto riguarda il sistema Google, gli strumenti utilizzati per la comunicazione sono:

Gmail: Posta elettronica

GDrive: Archiviazione nel Cloud

GClassroom: Sistema di eLearning scolastico

GMeet: Videoconferenze per seguire le lezioni sincrone, senza possibilità di generare video riunioni.

3.3 - BYOD

La presente ePolicy conterrà indicazioni, revisioni o eventuali integrazioni di Regolamenti già esistenti che disciplinano l'usodei dispositivi personali in classe, a seconda dei vari usi, anche in considerazione dei dieci punti del Miur per l'uso deidispositivi mobili a scuola (BYOD, "Bring your own device"). Risulta infatti fondamentale per la comunità scolastica aprire undialogo su questa tematica e riflettere sulle possibilità per l'Istituto di dotarsi di una regolamentazione condivisa e specificache tratti tali aspetti, considerando aspetti positivi ed eventuali criticità nella e per la didattica.

L'utilizzo della strumentazione personale è regolata in generale dal Regolamento sull'uso della rete Internet, delle apparecchiature e dei laboratori informatici, pubblicato sul sito web dell'istituto.

L'istituto ha approntato la modulistica specifica per la stipula di un patto di corresponsabilità digitale tra la scuola, le famiglie e gli studenti

In particolare sono previste le seguenti regole: Docenti:

I docenti fanno uso di dispositivi personali, solitamente tablet o laptop, più raramente smartphone, per le attività didattiche o per la preparazione delle stesse. Tuttavia l'Istituto mette a disposizione un certo numero di laptop per i docenti che ne fossero sprovvisti, anche temporaneamente. Essi accedono al registro elettronico per gli adempimenti di rito, come l'apposizione della firma delle ore di lezione svolte, l'inserimento delle valutazioni scritte, orali o pratiche assegnate agli studenti, per indicare le giornate e gli orari di colloquio con le famiglie che vengono svolti utilizzando Google Meet.

Studenti:

Come precedentemente indicato, gli studenti non hanno il permesso di accedere alla rete Internet, se non nel caso di uso della metodologia BYOD per progetti che lo prevedano; tuttavia, durante le lezioni gli studenti possono essere invitati dal docente ad utilizzare a fini didattici i dispositivi in loro possesso con connessioni ad internet fornite dagli abbonamenti della connettività alla rete di tipo personali.

ATA

Per il personale ATA solo gli assistenti amministrativi e gli assistenti tecnici sono autorizzati per l'accesso alla rete Wifi.

SOGGETTI ESTERNI

Per i soggetti esterni vengono approntate reti wifi ad hoc temporanee, per fornire accesso nel corso di eventi specifici, conferenze, esami di stato etc.

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 dilocandine da affiggere a scuola, attraverso news nel sito della scuola e durante i collegi docenti e attraverso tutti i canali maggiormente utili ad un'efficace comunicazione.

A seguire, le problematiche a cui fanno riferimento le procedure allegate:

Cyberbullismo: è necessario capire se si tratta effettivamente di cyberbullismo o di altra problematica. Oltre al contesto, vanno considerate le modalità attraverso le quali il comportamento si manifesta (alla presenza di un "pubblico"? Tra coetanei? In modo ripetuto e intenzionale? C'è un danno percepito alla vittima? etc.). È necessario poi valutare l'eventuale

stato di disagio vissuto dagli/lle studenti/esse coinvolti/e (e quindi valutare se rivolgersi ad un servizio deputato ad offrire un supporto psicologico e/o di mediazione).

Adescamento online: se si sospetta un caso di adescamento online è opportuno, innanzitutto, fare attenzione a non cancellare eventuali prove da smartphone, tablet e computer utilizzati dalla persona minorenne e inoltre è importante non sostituirsi al bambino/a e/o adolescente, evitando, quindi, di rispondere all'adescatore al suo posto). È fondamentale valutare il benessere psicofisico dei minori e il rischio che corrono. Vi ricordiamo che l'attuale normativa prevede che la persona coinvolta in qualità di vittima o testimone in alcune tipologie di reati, tra cui il grooming, debba essere ascoltata in sede di raccolta di informazioni con l'ausilio di una persona esperta in psicologia o psichiatria infantile.

Sexting: nel caso in cui immagini e/o video, anche prodotte autonomamente da persone minorenni, sfuggano al loro controllo e vengano diffuse senza il loro consenso è opportuno adottare sistemi di segnalazione con l'obiettivo primario di tutelare il minore e ottenere, 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.

Si suggeriscono, 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.

Gli studenti, i docenti e tutto il personale operante nella scuola possono segnalare al referente del cyberbullismo casi sospetti o evidenti di cyberbullismo, sexting, adescamento online, compilando l'apposita modulistica fruibile sia sul sito istituzionale della scuola sia presso il primo terra, al banco del personale ATA adiacente alla Vicepresidenza. Qualora la segnalazione avvenga tramite e-mail deve essere inviata all'indirizzo elettronico del referente del cyberbullismo rintracciabile sul sito scolastico.

CYBERBULLISMO

Per cyberbullismo si intende "qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno ai minorenni, realizzata per via telematica, nonché la diffusione di contenuti online aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale o predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la messa in ridicolo" (L.71/2017)

Si possono configurare come reati di cyberbullismo:

Flaming: litigi on line nei quali si fa uso di un linguaggio violento e volgare.

Harassment: molestie attuate attraverso l'invio ripetuto di linguaggi offensivi.

Cyberstalking: invio ripetuto di messaggi che includono esplicite minacce fisiche, al punto che la vittima arriva a

temere per la propriaincolumità.

Denigrazione: pubblicazione all'interno di comunità virtuali, quali newsgroup, blog, forum di discussione, messaggistica immediata, siti internet, ecc, di pettegolezzi e commenti crudeli, calunniosi e denigratori.

Outing estorto: registrazione delle confidenze – raccolte all'interno di un ambiente privato creando un clima di fiducia e poi inserite integralmente in un blog pubblico.

Impersonificazione: insinuazione all'interno dell'account di un'altra persona con l'obiettivo di inviare dal medesimo messaggi ingiuriosiche screditino la vittima.

Esclusione: estromissione intenzionale dall'attività on line.

ADESCAMENTO ONLINE

Per Adescamento online si intende "qualsiasi atto volto a carpire la fiducia di un minorenne (minore di 16 anni) attraverso espedienti, promesse o minacce, anche mediante l'utilizzo della Rete o di altri mezzi di comunicazione, al fine di commettere i reati di riduzione o mantenimento in schiavitù o in servitù, prostituzione minorile, pornografia minorile, detenzione di materiale pedopornografico, iniziative turistiche volte allosfruttamento della prostituzione minorile, violenza sessuale, atti sessuali con minorenni, corruzione di minorenne, violenza sessuale di gruppo" (art. 609 undecies del C.P.). In sintesi, trattasi di un lungo processo avviato da un adulto abusante che usa le nuove tecnologie per cercarecontatti, manipolare psicologicamente dei minori al fine di costruire delle relazioni pseudo sentimentali finalizzate a indurre e coinvolgere minori in azioni sessuali reali e/o tecnomediate.

SEXTING

Per Sexting si intende la pratica di inviare, postare o condividere messaggi di testo, immagini e/o video a sfondo sessuale, via cellulare o tramite Internet. Le immagini e i video possono ritrarre la vittima nuda o seminuda o in atteggiamenti a sfondo erotico. Tale azione si configura come reato se:

- l'adulto incita il/la minore di anni 18 all'invio del suddetto materiale, anche qualora il/la minore sia consensuale
- l'adulto invia il suddetto materiale al/alla minore di anni 18 anni.

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 minorenne.

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.

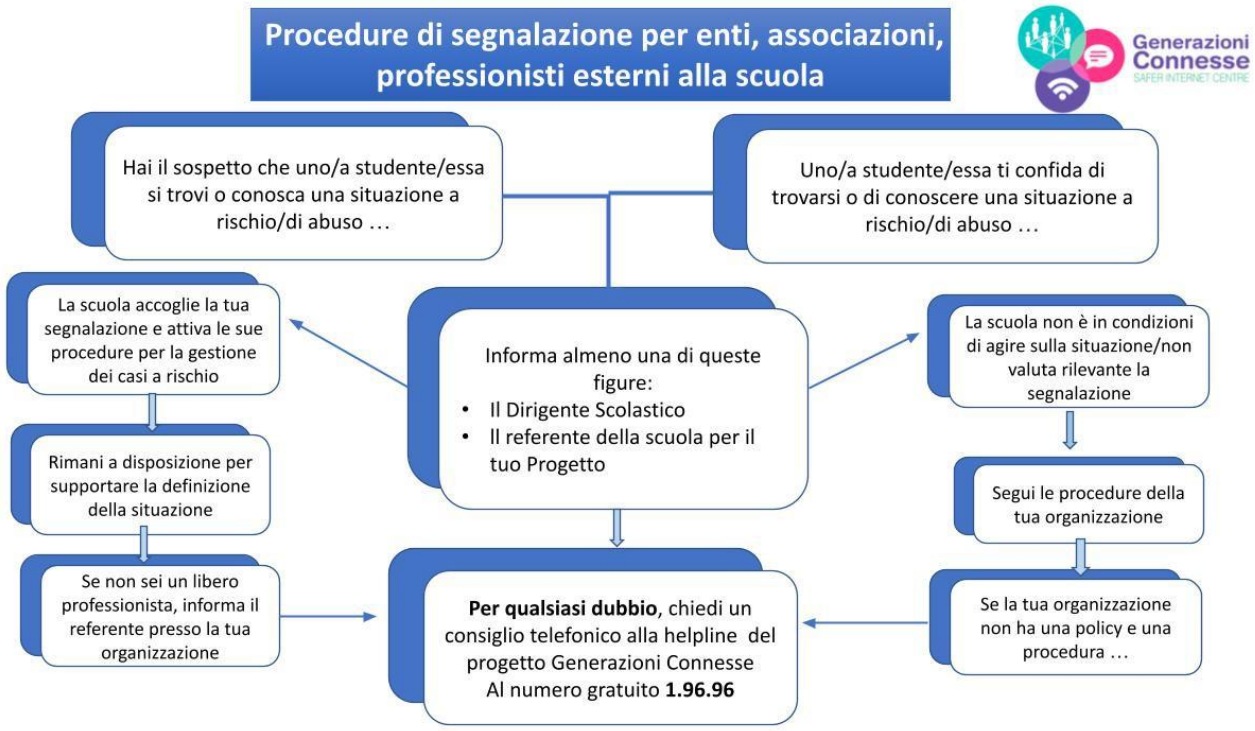
Strumenti a disposizione di studenti/esse

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.

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 alPTOF.

Schema delle procedure scolastiche in caso di atti di bullismo e cyberbullismo



Procedure interne: cosa fare in caso di evidenza di Cyberbullismo

Generazioni Connesse SAFER INTERNET CENTRE

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 condividete 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.

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).

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.

Procedure interne: cosa fare in caso di sospetto di Cyberbullismo

Generazioni Connesse SAFER INTERNET CENTRE

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

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.

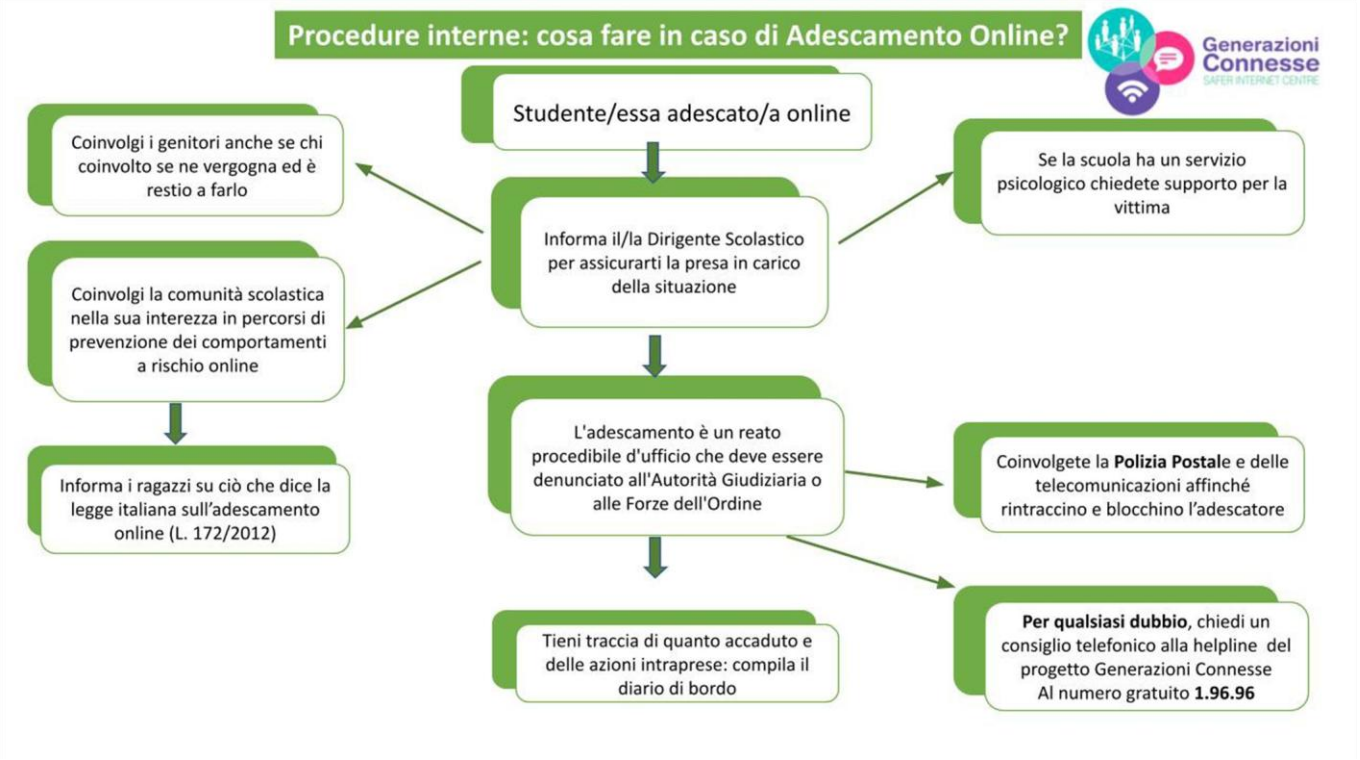
Se emergono evidenze passa allo schema successivo

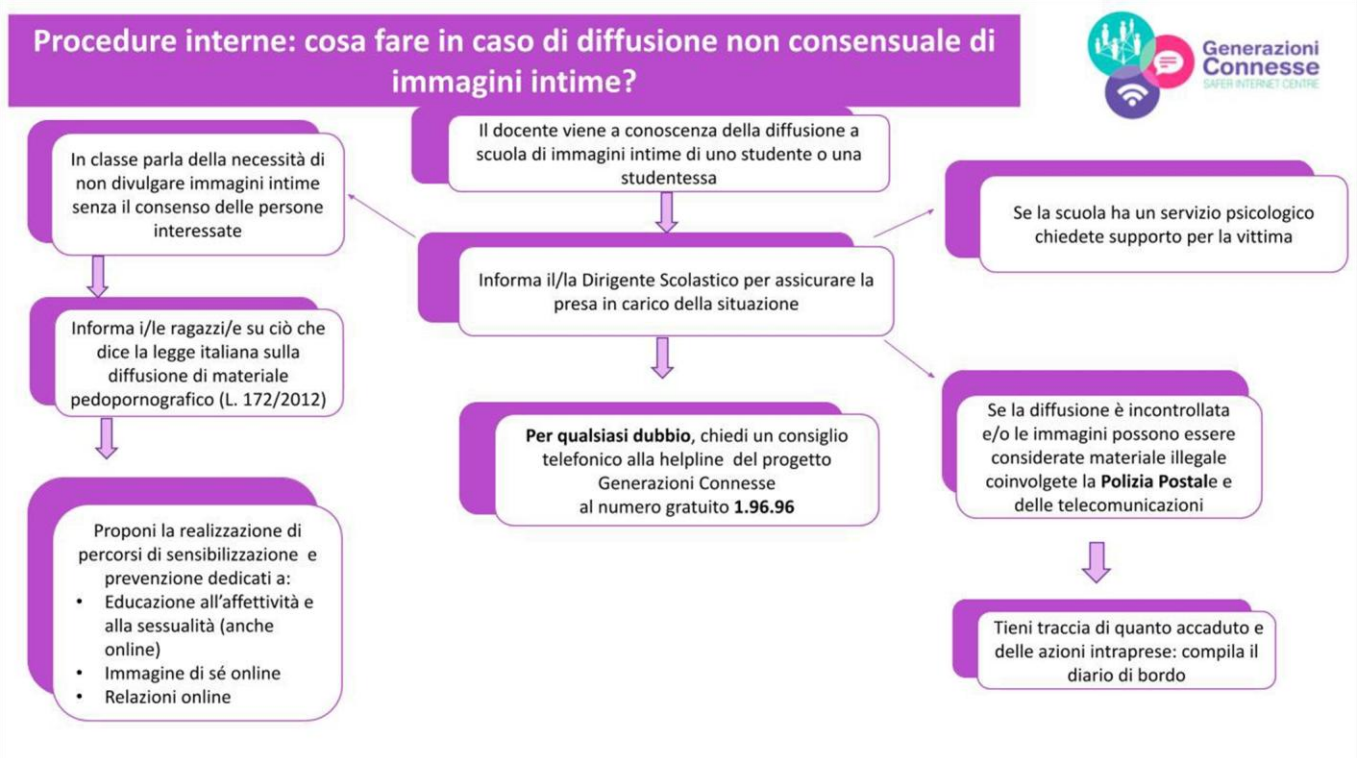
Se, come docente, hai un dubbio su come procedere o interpretare quello che sta accadendo, puoi chiedere in qualsiasi momento, una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

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

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

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


Procedure interne: cosa fare in caso di Adescamento Online?
Generazioni Connesse
Studente/essa adescato/a online
Coinvolgi i genitori anche se chi coinvolto se ne vergogna ed è restio a farlo
Coinvolgi la comunità scolastica nella sua interezza in percorsi di prevenzione dei comportamenti a rischio online
Informa i ragazzi su ciò che dice la legge italiana sull'adescamento online (L. 172/2012)
Informa il/la Dirigente Scolastico per assicurarti la presa in carico della situazione
Se la scuola ha un servizio psicologico chiedete supporto per la vittima
L'adescamento è un reato procedibile d'ufficio che deve essere denunciato all'Autorità Giudiziaria o alle Forze dell'Ordine
Coinvolgete la Polizia Postale e delle telecomunicazioni affinché rintraccino e blocchino l'adescatore
Tieni traccia di quanto accaduto e delle azioni intraprese: compila il diario di bordo
Per qualsiasi dubbio, chiedi un consiglio telefonico alla helpline del progetto Generazioni Connesse Al numero gratuito 1.96.96


Procedure interne: cosa fare in caso di diffusione non consensuale di immagini intime?
Generazioni Connesse
In classe parla della necessità di non divulgare immagini intime senza il consenso delle persone interessate
Informa i/le ragazzi/e su ciò che dice la legge italiana sulla diffusione di materiale pedopornografico (L. 172/2012)
Proponi la realizzazione di percorsi di sensibilizzazione e prevenzione dedicati a:
• Educazione all'affettività e alla sessualità (anche online)
• Immagine di sé online
• Relazioni online
Il docente viene a conoscenza della diffusione a scuola di immagini intime di uno studente o una studentessa
Informa il/la Dirigente Scolastico per assicurare la presa in carico della situazione
Per qualsiasi dubbio, chiedi un consiglio telefonico alla helpline del progetto Generazioni Connesse al numero gratuito 1.96.96
Se la scuola ha un servizio psicologico chiedete supporto per la vittima
Se la diffusione è incontrollata e/o le immagini possono essere considerate materiale illegale coinvolgete la Polizia Postale e delle telecomunicazioni
Tieni traccia di quanto accaduto e delle azioni intraprese: compila il diario di bordo

La diffusione delle procedure per la segnalazione di casi sospetti o accertati di cyberbullismo saranno prossimamente pubblicate sia nel sito istituzionale sia all'interno della scuola mediante l'affissione di apposite locandine in punti strategici dell'Istituto poiché è dovere di tutto il personale operante nella scuola segnalare i casi. Tali procedure sono contenute anche nel Protocollo per la prevenzione del bullismo e del cyberbullismo, recentemente aggiornato e che sarà anch'esso condiviso con la comunità scolastica e le famiglie nel sito istituzionale.

I docenti e il personale operante all'interno della scuola rivestono la qualifica di Pubblico Ufficiale come da art.357 del Codice Penale 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.

Ciò è di fondamentale importanza nel momento in cui l'insegnante si confronta con un caso di comportamento online a rischio e quindi ha la responsabilità di segnalare tale situazione.

Di seguito si riportano le procedure che l'Istituto mette in atto:

EPISODIO SOSPETTO

In presenza di un episodio **sospetto** di cyberbullismo, sexting, adescamento online ecc. è cruciale che il personale scolastico intervenga tempestivamente segnalando in modo dettagliato il caso al referente per il cyberbullismo, mediante l'apposita modulistica predisposta dalla scuola, fruibile in versione online sul sito della scuola o in versione cartacea al banco del personale ATA adiacente alla vicepresidenza, al primo piano.

Il referente per il cyberbullismo, una volta raccolta la segnalazione, entro due giorni dalla ricezione, la condivide con ilDirigente scolastico, per una prima valutazione dell'evento.

Il referente del cyberbullismo, allo stesso tempo, si confronta con i docenti della classe, cooperando con il coordinatore della stessa, raccoglie maggiori informazioni sul caso (valutazione approfondita) anche avvalendosi dello psicologo dell'istituto, individua le possibili azioni da intraprendere e le condivide con i docenti della classe. Attraverso questa seconda fase il docente referente del cyberbullismo può valutare il livello di rischio di bullismo e vittimizzazione per meglio definire le procedure da seguire.

Definito il livello di rischio, il referente del cyberbullismo e il Dirigente scolastico decidono in merito all'approccio educativo con la classe, ai colloqui individuali con la/e vittima/e e il/i cyberbullo/i, all'intervento dello psicologo scolastico per analizzare più accuratamente la situazione ed eventuali sintomi nel/i cyberbullo/i e nella/e vittima/e. A seguito di questi primi interventi, si deciderà in merito all'attuazione di un incontro tra vittima/e e bullo/i per la gestione della relazione.

Inoltre, il Dirigente scolastico, accertata la presenza di un caso di cyberbullismo ha l'obbligo di convocare i genitori o i tutori degli alunni coinvolti, eventualmente con il supporto dell'operatore dello sportello psicologico (L.71/2017).

EPISODIO DI EVIDENZA

Nel caso di un episodio di **evidenza**, il personale scolastico, una volta venuto a conoscenza di un caso certo di cyberbullismo, come nella procedura precedente, ha l'obbligo di intervenire tempestivamente segnalando, in modo dettagliato e mediante apposita modulistica, il caso al referente per il cyberbullismo il quale la discute e condivide, al massimo entro due giorni, con il Dirigente Scolastico.

REATI PERSEGUIBILI D'UFFICIO

Nei casi di **reati perseguibili d'ufficio** (per es. sexting, pedopornografia, adescamento on-line…) o se si sospetta gravepregiudizio per il minore, il personale scolastico che ne abbia avuto notizia, ne dà immediata comunicazione al referente del cyberbullismo. Il referente si rivolge immediatamente al Dirigente Scolastico che presenta denuncia

all'autorità competente, mediante compilazione dell'apposita modulistica, presente nelle *Linee di orientamento per la prevenzione e il contrasto deifenomeni di Bullismo e Cyberbullismo*, aggiornate con decreto n.18 del 13/01/2021 e relativa nota (modulistica reperibile sulsito dell'Istituto).

Il Dirigente scolastico è tenuto senza indugio a denunciare all'autorità giudiziaria competente. La denuncia in forma scritta è d'obbligo anche nell'ipotesi in cui sia diretta contro ignoti.

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.

Anche nei casi di evidenza di episodi di cyberbullismo, sexting, adescamento online il Dirigente può proporre incontri individuali con la/le vittima/e, incontri individuali con il/i bullo/i e incontri alla presenza di entrambe le parti coinvolte.

L'ITER CONSIGLIATO

"In generale, in caso di episodio sospetto e/o denunciato, si suggerisce di seguire il seguente schema di intervento come daLinee 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."

La convocazione dei genitori non deve essere fatta per i reati di sexting, pedopornografia o per altri reati in cui sia possibile che la vulnerabilità del minore nasca all'interno del nucleo familiare.

A CHI POSSONO RIVOLGERSI GLI STUDENTI

Gli studenti, che vivano in prima persona o come testimoni situazioni problematiche, possono rivolgersi ai docenti del Consiglio di classe, al Dirigente Scolastico, al referente per il contrasto del bullismo e del cyberbullismo, e/o allo psicologo operante all'interno dell'Istituto, a qualsiasi Commissariato di P.S., al Commissariato on-line (https://www.commissariatodips.it/), alla Polizia Postale, all'Arma dei Carabinieri.

Inoltre, gli studenti possono inviare la propria segnalazione, anche in forma anonima, tramite l'applicazione You Pol della Polizia di Stato.

(https://www.poliziadistato.it/statics/40/presentazione_youpol_-esserci.pdf.pdf).

In particolare, i minori che ritengano che determinati contenuti a loro riferiti e diffusi per via telematica (foto e/o video imbarazzanti e/o offensivi, pagine web e/o post sui social network in cui si è vittime di minacce e/o offese e/o insulti, ecc.) siano atti di cyberbullismo, sexting ecc. ne possono richiedere l'oscuramento, la rimozione o il blocco. Le richieste vanno inviate al titolare del trattamento o al gestore del sito o del social media dove sono pubblicati tali contenuti. L'istanza può essere inoltrata direttamente dal minore ultraquattordicenne, oppure da chi esercita la responsabilità genitoriale. Nel caso la richiesta non venga soddisfatta, ci si può rivolgere al Garante per la protezione

dei dati personali che, entro 48 ore, provvede in merito alla segnalazione (L.71/2017). Per inoltrare le segnalazioni si può utilizzare il modello disponibile su www.garanteprivacy.it/cyberbullismo, inviandolo via e-mail a cyberbullismo@gpdp.it.

Lo studente nel momento in cui segnala il caso di cyberbullismo alla scuola è chiamato a compilare il modulo per la segnalazione in ogni sua parte. Tale modulo, fruibile online sul sito della scuola o in cartaceo al primo piano, presso il banco del personale ATA adiacente alla vicepresidenza, deve essere inoltrato in busta chiusa al referente del cyberbullismo e deveessere compilato in modo dettagliato in ogni sua parte. Qualora lo studente decida di inoltrare la segnalazione via e mail puòinviarla all'indirizzo del referente del cyberbullismo.

Lo psicologo operante all'interno dell'Istituto scolastico, gli esperti esterni coinvolti in azioni di docenza per attivitàdell'Istituto (progetti, PCTO, corsi …), in sede o fuori sede, ricoprono il ruolo di Operatori Incaricati di Pubblico Servizio (art.358 c.p.) e come tali sono obbligati a denunciare e/ o segnalare i fatti appartenenti alle tipologie sopra descritte, di cui sono informati per testimonianza diretta o visione diretta di materiale che rientri nelle categorie di reati precedentemente indicati. Pertanto, sono tenuti a mettere in atto le procedure contenute nei precedenti paragrafi, comunicando, inoltre, per iscritto, al docente con cui abitualmente hanno contatti (referente di progetto, coordinatore di classe, docente dellaclasse,…), i fatti di cui sono venuti a conoscenza e l'avvenuta segnalazione al referente del cyberbullismo, e/o al Dirigente Scolastico e/o all'autorità di P.S. e/o all'autorità giudiziaria.

Il Consiglio di classe a cui appartenga lo studente o il gruppo di studenti coinvolto nei fatti, previa informativa da parte deltitolare della segnalazione/denuncia o da parte del Dirigente Scolastico, attiva percorsi di informazione, prevenzione e sensibilizzazione, avvalendosi, se giudicato opportuno, del supporto di esperti esterni quali lo psicologo di istituto, servizi sociali, forze dell'ordine, Polizia Postale, ecc.

E' fondamentale che venga rispettato il segreto d'ufficio sull'identità dei soggetti implicati, indipendentemente dal loro ruolo.

In tutte queste procedure, gli studenti, le famiglie, il Dirigente Scolastico, i docenti, il personale ATA, gli esperti esterni possono avvalersi della collaborazione del referente per il contrasto al bullismo e al cyberbullismo.