Documento di ePolicy

BAIC85800B

I.C. "G. MINZELE - G. PARINI"

VIA PETRUZZI 18 - 70017 - PUTIGNANO - BARLETTA-ANDRIA-TRANI (BA)

Francesco Tricase

Capitolo 1 - Introduzione al documento di ePolicy

1.1 - Scopo dell'ePolicy

Le TIC (Tecnologie dell'informazione e della comunicazione) rappresentano strumenti fondamentali nel processo educativo e per l'apprendimento degli studenti e delle studentesse.

Le "competenze digitali" sono fra le abilità chiave all'interno del Quadro di riferimento Europeo delle Competenze per l'apprendimento permanente e di esse bisogna dotarsi proprio a partire dalla scuola (Raccomandazione del Consiglio Europeo del 2006 aggiornata al 22 maggio 2018, relativa alle competenze chiave per l'apprendimento permanente).

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

L'E-policy ha l'obiettivo di esprimere la nostra visione educativa e proposta formativa, in riferimento alle tecnologie digitali. Nello specifico:

- l'approccio educativo alle tematiche connesse alle "competenze digitali", alla privacy, alla sicurezza online e all'uso delle tecnologie digitali nella didattica e nel percorso educativo;
- le norme comportamentali e le procedure di utilizzo delle Tecnologie dell'Informazione e della Comunicazione (ICT) in ambiente scolastico;
- le misure per la prevenzione e la sensibilizzazione di comportamenti on-line a rischio;
- le misure per la rilevazione, segnalazione e gestione delle situazioni rischiose legate ad un uso non corretto delle tecnologie digitali.

Argomenti del Documento

1. **Presentazione dell'ePolicy**
    1. Scopo dell'ePolicy
    2. Ruoli e responsabilità
    3. Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto
    4. Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica

5. Gestione delle infrazioni alla ePolicy
6. Integrazione dell'ePolicy con regolamenti esistenti
7. Monitoraggio dell'implementazione dell'ePolicy e suo aggiornamento

2. **Formazione e curricolo**
    1. Curricolo sulle competenze digitali per gli studenti
    2. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica
    3. Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali
    4. Sensibilizzazione delle famiglie e Patto di corresponsabilità
3. **Gestione dell'infrastruttura e della strumentazione ICT (Information and Communication Technology) della e nella scuola**
    1. Protezione dei dati personali
    2. Accesso ad Internet
    3. Strumenti di comunicazione online
    4. Strumentazione personale
4. **Rischi on line: conoscere, prevenire e rilevare**
    1. Sensibilizzazione e prevenzione
    2. Cyberbullismo: che cos'è e come prevenirlo
    3. Hate speech: che cos'è e come prevenirlo
    4. Dipendenza da Internet e gioco online
    5. Sexting
    6. Adescamento online
    7. Pedopornografia
5. **Segnalazione e gestione dei casi**
    1. Cosa segnalare
    2. Come segnalare: quali strumenti e a chi
    3. Gli attori sul territorio per intervenire
    4. Allegati con le procedure

Perché è importante dotarsi di una E-policy?

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

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

L'IC Minzele Parini, seguendo le indicazioni delle Linee d'orientamento per azioni di prevenzione e di contrasto al bullismo e cyberbullismo, elaborate, nell'ottobre 2019, dal Ministero dell'Istruzione,

dell'Università e della Ricerca, in collaborazione con "Generazioni Connesse" e il Safer Internet Center per l'Italia, elabora questo documento di E-Safety Policy.
L'intento è quello di formare e sensibilizzare non soltanto gli studenti, ma anche il corpo docente, amministrativo ed i genitori ad un utilizzo sicuro e davvero consapevole di internet e delle relative risorse.

1.2 - Ruoli e responsabilità

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

Ciascuna delle figure professionali che, a vario titolo, si occupano di gestione e programmazione delle attività formative, didattiche ed educative dell'Istituto, infatti, deve conoscere le responsabilità legate al proprio ruolo.

Il **Dirigente scolastico**, al fine di promuovere l'uso consentito delle tecnologie e di Internet, deve assolvere ai seguenti compiti:

- garantire una formazione adeguata del personale docente relativo all'uso delle TIC nella didattica;
- garantire la sicurezza (tra cui la sicurezza on-line) dei membri della comunità scolastica, mediante sistemi di monitoriaggio e controllo;
- promuovere la cultura della sicurezza online e fornire il proprio contributo all'organizzazione, insieme al docente referente sulle tematiche del bullismo/cyberbullismo, di corsi di formazione specifici per tutte le figure scolastiche sull' utilizzo positivo e responsabile delle TIC;
- gestire ed intervenire nei casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali.

L'**Animatore digitale**, supportato dal Team dell'innovazione, deve:

- farsi promotore di percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale", con attenzione particolare allo sviluppo di competenze digitali nell'ambito dell'educazione alla cittadinanza;
- supportare il personale della scuola dal punto di vista recnico-informatico;
- fornire consulenza e informazioni al personale in relazione ai rischi on-line e alle misure di prevenzione e gestione dei dati personali;
- monitorare e rilevare eventuali episodi o problematiche connesse all'uso delle TIC a scuola;
- controllare che gli utenti autorizzati accedano alla Rete della scuola con apposita password, per scopi istituzionali e consentiti (istruzione e formazione);
- curare la manutenzione e lo sviluppo del sito web della scuola;

- coinvolgere la comunità scolastica (alunni, genitori e altri attori del territorio) nella partecipazione ad attività e progetti attinenti la "scuola digitale.

Il **Referente bullismo e cyberbullismo**, figura individuata nell'Art. 4 Legge n.71/2017, deve:

- coordinare e promuovere iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo; a tal fine, può avvalersi della collaborazione delle Forze di polizia, delle associazioni e dei centri di aggregazione giovanile del territorio;
- coinvolgere, con progetti e percorsi formativi ad hoc, studenti, colleghi e genitori.

I **Docenti** tutti devono:

- informarsi/aggiornarsi sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di internet e sulla politica di sicurezza adottata dalla scuola, rispettandone il regolamento;
- diffondere la cultura dell'uso responsabile delle TIC e della Rete;
- integrare parti del curriculum della propria disciplina con approfondimenti ad hoc, promuovendo, laddove possibile, anche l'uso delle tecnologie digitali nella didattica;
- accompagnare e supportare gli studenti e le studentesse nelle attività di apprendimento e nei laboratori che prevedono l'uso della LIM o di altri dispositivi tecnologici che si connettono alla Rete;
- segnalare al Dirigente Scolastico qualunque problematica, violazione o abuso, anche online, che vede coinvolti studenti e studentesse.

Il **personale Amministrativo, Tecnico e Ausiliario (ATA)** dovrebbe:

- essere coinvolto nella segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo;
- insieme ad altre figure raccogliere, verificare e valutare le informazioni inerenti possibili casi di bullismo/cyberbullismo.

Studenti e Studentesse:

- dovrebbero, 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;
- dovrebbero 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 **Genitori**, in continuità con l'Istituto scolastico, dovrebbero:

- essere partecipi e attivi nelle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete, nonché sull'uso responsabile dei device personali;
- relazionarsi in modo costruttivo con i docenti sulle linee educative che riguardano le TIC e la Rete e comunicare con loro circa i problemi rilevati quando i/le propri/e figli/e non usano responsabilmente le tecnologie digitali o Internet;

- accettare e condividere quanto scritto nell'ePolicy dell'Istituto.

Gli **Enti educativi esterni e le associazion**i che entrano in relazione con la scuola dovrebbero

- conformarsi alla politica della stessa riguardo all'uso consapevole della Rete e delle TIC;
- promuovere comportamenti sicuri, la sicurezza online e assicurare la protezione degli studenti e delle studentesse durante le attività che si svolgono insieme.

1.3 - Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto

Tutti gli attori che entrano in relazione educativa con gli studenti e le studentesse devono: mantenere sempre un elevato profilo personale e professionale, eliminando atteggiamenti inappropriati, essere guidati dal principio di interesse superiore del minore, ascoltare e prendere in seria considerazione le opinioni ed i desideri dei minori, soprattutto se preoccupati o allertati per qualcosa.

Sono vietati i comportamenti irrispettosi, offensivi o lesivi della privacy, dell'intimità e degli spazi personali degli studenti e delle studentesse oltre che quelli legati a tollerare o partecipare a comportamenti di minori che sono illegali, o abusivi o che mettano a rischio la loro sicurezza.

Tutti gli attori esterni sono tenuti a conoscere e rispettare le regole del nostro Istituto dove sono esplicitate le modalità di utilizzo dei propri dispositivi personali (smartphone, tablet, pc, etc.) e quelli in dotazione della scuola, evitando un uso improprio o comunque deontologicamente scorretto durante le attività con gli studenti e le studentesse. Esiste l'obbligo di rispettare la privacy, soprattutto dei soggetti minorenni, in termini di fotografie, immagini, video o scambio di contatti personali (numero, mail, chat, profili di social network).

Al fine di rendere l'ePolicy uno strumento efficace per la tutela degli studenti e delle studentesse, intesa in senso ampio, viene individuato un insieme di regole o norme di comportamento da condividere con le organizzazioni/associazioni extrascolastiche e gli esperti esterni chiamati, a vario titolo, alla realizzazione di progetti ed attività educative, sul breve e/o lungo periodo.

Dotarsi di un'informativa sintetica sull'ePolicy comprensiva delle procedure di segnalazione da condividere con tutte le figure che operano con studenti e studentesse, significa non solo tutelare questi ultimi e la scuola stessa, ma anche porre in essere nuove modalità per rilevare, limitare e contrastare possibili pericoli legati a condotte educative non professionali.

È importante garantire che tutti i soggetti esterni che erogano attività in ambito scolastico siano

sensibilizzati e resi consapevoli dei rischi online che possono correre gli studenti e le studentesse e dei comportamenti corretti che devono adottare a scuola.

1.4 - Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica

Il documento di E-policy viene condiviso con tutta la comunità educante, ponendo al centro gli studenti e le studentesse e sottolineando compiti, funzioni e attività reciproche. È molto importante che ciascun attore scolastico (dai docenti agli/lle studenti/esse) si faccia a sua volta promotore del documento.

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

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

Il documento è approvato dal Collegio dei Docenti e dal Consiglio di Istituto e viene esposto in versione semplificata negli spazi che dispongono di pc collegati alla Rete o comunque esposto in vari punti spaziali dell'Istituto.

Gli studenti e le studentesse vengono informati sul fatto che sono monitorati e supportati nella navigazione on line, negli spazi della scuola e sulle regole di condotta da tenere in Rete.

La scuola si impegna a redigere una versione child friendly del documento per la comunicazione e la sensibilizzazione ai/lle bambini/e e ai/lle ragazzi/e. Nella comunicazione e condivisione dell'ePolicy è importante, infatti, valutare i vari target di riferimento (studenti/studentesse, docenti, genitori, personale amministrativo, collaboratori scolastici etc.) individuando di conseguenza i linguaggi, le modalità e i canali di comunicazione e condivisione più adatti.

1.5 - Gestione delle infrazioni alla ePolicy

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

Alcune possibili condotte sanzionabili, in relazione all'uso improprio delle TIC e della Rete a scuola da parte degli studenti e delle studentesse, sono le seguenti:

- la condivisione online di immagini o video di compagni/e senza il loro consenso o che li ritraggono in pose offensive e denigratorie;
- la condivisione di scatti intimi e a sfondo sessuale; la condivisione di dati personali; l'invio di immagini o video volti all'esclusione di compagni/e.

A seconda dell'età dello studente o della studentessa, è molto importante intervenire su tutto il contesto classe con attività specifiche educative e di sensibilizzazione, allo scopo di promuovere una maggior consapevolezza circa l'utilizzo delle TIC e di Internet.

Le infrazioni della policy posso essere rilevate dai docenti, dagli ATA, durante l'esercizio delle proprie funzioni, dagli alunni e dai genitori.

Qualora venga individuata un'inosservanza, è necessario informare il coordinatore di classe, il quale a sua volta riferirà al Dirigente Scolastico e alla famiglia. Nel caso in cui l'infrazione si configuri come atto di cyberbullismo, il docente informa il referente per il bullismo/cyberbullismo. Nel caso si tratti di un reato è necessario che il Dirigente informi le autorità competenti (polizia postale).

1.6 - Integrazione dell'ePolicy con Regolamenti esistenti

Il Regolamento dell'Istituto Scolastico viene aggiornato con specifici riferimenti all'E-policy, così come anche il Patto di Corresponsabilità, in coerenza con le Linee Guida Miur e le indicazioni normative generali sui temi in oggetto.

Quanto contenuto nel documento E-policy della scuola risulta in linea con le disposizioni del Regolamento di Istituto aggiornato per il triennio 2019-2022.

Si riassume quanto segue, in riferimento alla Sezione V- Doveri degli alunni- Norme di comportamento e Discipline, per cui si rimanda al sottoparagrafo specifico dedicato all'utilizzo dei cellulari e dei dispositivi a scuola.

Secondo quanto stabilito nel Regolamento, il docente che ha rilevato l'infrazione procederà ad informare il D. S. il quale, anche ai fini dell'applicazione degli artt. 161 e 166 del D.lgs. 196/2003, mette a conoscenza dei soggetti ripresi della avvenuta violazione e valuta, unitamente ai colleghi del Consiglio di Classe / Interclasse, l'opportunità di irrogare una sanzione disciplinare e la relativa entità.

Sono previsti i seguenti provvedimenti disciplinari:

- richiamo verbale;
- richiamo scritto sul registro di classe o con annotazione sul diario;
- convocazione dei genitori da parte degli insegnanti.;
- convocazione dei genitori da parte del Dirigente scolastico.

In presenza di situazioni e/o episodi gravi, il Dirigente Scolastico provvederà alle opportune segnalazioni alle autorità competenti secondo le indicazioni della legge 71.2017. 2.

1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

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

Il Dirigente Scolastico è responsabile dell'implementazione della policy all'interno dell'Istituto. L'Animatore Digitale, insieme al Team dell'innovazione digitale e al Referente per il Bullismo e il Cyberbullismo, in accordo con il Dirigente Scolastico, partecipano alla revisione e all'aggiornamento del documento. L'aggiornamento del documento viene sottoposto all'approvazione del Collegio dei Docenti e del Consiglio di Istituto.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

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

Azioni da svolgere nei prossimi 3 anni:

- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto agli

studenti

- Organizzare 1 evento di presentazione e conoscenza dell’ePolicy rivolto ai docenti
- Organizzare 1 evento di presentazione e conoscenza dell’ePolicy rivolto ai genitori

Capitolo 2 - Formazione e curricolo

2.1. Curricolo sulle competenze digitali per gli studenti

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

Infatti, “la competenza digitale presuppone l’interesse per le tecnologie digitali e il loro utilizzo con dimestichezza e spirito critico e responsabile per apprendere, lavorare e partecipare alla società. Essa comprende l’alfabetizzazione informatica e digitale, la comunicazione e la collaborazione, l’alfabetizzazione mediatica, la creazione di contenuti digitali (inclusa la programmazione), la sicurezza (compreso l’essere a proprio agio nel mondo digitale e possedere competenze relative alla cybersicurezza), le questioni legate alla proprietà intellettuale, la risoluzione di problemi e il pensiero critico” (“Raccomandazione del Consiglio europeo relativa alla competenze chiave per l’apprendimento permanente”, C189/9, p.9).

Per questo la scuola si impegna a portare avanti percorsi volti a promuovere tali competenze, al fine di educare gli studenti e le studentesse verso un uso consapevole e responsabile delle tecnologie digitali. Ciò avverrà attraverso la progettazione e implementazione di un curricolo digitale.

Con riferimento al Piano Nazionale della Scuola Digitale, l'IC Minzele Parini si impegna a promuovere una serie di competenze digitali di base, trasversali alle diverse discipline, che permettano agli studenti, al termine dei due cicli di scuola Primaria e Secondaria di primo grado, di utilizzare in maniera consapevole e responsabile le più comuni tecnologie dell’informazione e della comunicazione per elaborare ed archiviare dati, testi e immagini, per produrre documenti e semplici presentazioni, per reperire e condividere in rete informazioni e materiali di studio; si propone inoltre di sviluppare attività che mirino all’educazione alla sicurezza online e alla sensibilizzazione ai rischi di un uso improprio delle TIC e della rete, con particolare attenzione ai fenomeni crescenti di cyberbullismo, sexting, grooming. Questa esigenza, già emersa in precedenza, si rileva tanto più impellente in seguito all'esperienza della Didattica a Distanza, che ha evidenziato punti di forza e criticità nell'uso delle tecnologie e della Rete, ma anche nella produzione e creazione di semplici contenuti multimediali. Per questo motivo, risulta necessario elaborare un curricuolo digitale trasversale più dettagliato, al fine di favorire il consolidamento delle competenze di base.

La scuola si pone come obiettivo di sviluppare negli studenti le seguenti competenze:

- Conoscere e collegare le periferiche di input e output dei diversi dispositivi tecnologici presenti nella scuola (tastiera, mouse, scanner, schermo del PC, schermo LIM, audio, stampante, ecc.)
- Creare e spostare cartelle
- Creare e modificare documenti di scrittura, inserire immagini
- Creare e modificare altri tipi di documenti in base alle proposte didattiche delle diverse discipline (immagini, video, fogli di calcolo, presentazioni in Power Point, documenti di Geogebra, mappe create con Cmap o Mappe SuperEvo, Ipertesti ecc.)
- Archiviare correttamente i documenti creati nel PC (in apposite cartelle) e in altri dispositivi mobili (chiave USB, CD, DVD)
- Stampare un documento
- Utilizzare Internet per reperire informazioni funzionali allo studio con la consapevolezza che sia necessario verificare sempre se la fonte da cui si sta attingendo l'informazione sia attendibile
- Acquisire criteri per verificare l'attendibilità di una fonte Conoscere e rispettare le norme relative ai copyright, consapevoli delle sanzioni che derivano da un utilizzo non appropriato dei materiali reperiti in rete
- Conoscere i principali canali di condivisione delle informazioni (piattaforme on-line, chat, blog, social network)
- Essere consapevoli che l'identità digitale di coloro con cui condividiamo le informazioni on-line potrebbe non coincidere con quella reale. Diffidare quindi delle "amicizie" on-line con soggetti sconosciuti.
- Conoscere i fenomeni del cyberbullismo, sexting, grooming
- Conoscere il codice etico da rispettare on-line ed essere consapevoli delle conseguenze di comportamenti inadeguati
- Saper individuare e segnalare agli adulti di riferimento comportamenti inadeguati osservati in rete, specialmente se reiterati nel tempo
- Essere consapevoli dei rischi connessi alla pubblicazione on-line di foto, video e dati personali propri e di altri (chat, social network, YouTube, ecc.)
- Essere consapevoli delle possibili conseguenze legali connesse allo scaricare file senza permesso (come video e file musicali) e/o con contenuti inopportuni
- Essere consapevoli dei rischi per la salute fisica e psicologica di un utilizzo eccessivo, non regolamentato e non appropriato delle TIC (nuove dipendenze da internet)

2.2 - Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione)

nella didattica

È fondamentale che i docenti tutti siano formati ed aggiornati sull'uso corretto, efficace ed efficiente delle TIC nella didattica, al fine di usarle in modo integrativo ed inclusivo.

Ciò si rende necessario per fornire agli studenti e alle studentesse modelli di utilizzo positivo, critico e specifico delle nuove tecnologie e per armonizzare gli apprendimenti.

L'istituto si preoccupa, in coerenza con quanto affermato nel PTOF 2019/2022, di incrementare la formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica attraverso le seguenti azioni:
• Individuazione e formazione di un animatore digitale che accompagna il Dirigente Scolastico e il DSGA nell'attuazione degli obiettivi e delle innovazioni previste dal PNSD
• Supporto da parte di un Team, già esistente, per l'innovazione, composto da docenti e personale ATA, che collaborino con l'Animatore digitale e le funzioni strumentali dell'Area 5 nella promozione della didattica multimediale, coadiuvati anche dal pronto soccorso tecnico
• Corsi di formazione e aggiornamento interni e esterni all'Istituto su programmi e software specifici relativi alle singole discipline e/o volti all'acquisizione di competenze digitali trasversali.

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

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

L'Istituto propone di ampliare la formazione dei docenti sull'utilizzo consapevole di Internet e delle tecnologie digitali nei seguenti modi:

- Partecipazione al progetto Generazioni connesse e agli eventi indicati in relazione al Safer internet (es. Safer internet day)
- Iscrizione del Referente del Cyberbullismo alla Piattaforma ELISA (Formazione in E-Learning degli Insegnanti sulle Strategie Antibullismo), raccolta del materiale fornito dal corso in una banca dati accessibile a tutto il corpo docente
- Momenti di riflessione condivisa nei vari gruppi di lavoro

- Corsi di formazione interni all'istituto
- Autoformazione e formazione a distanza
- Partecipazione a incontri e corsi con esperti

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

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

La scuola avrà cura di sensibilizzare le famiglie sull'utilizzo consapevole delle TIC e della rete con particolare attenzione alle situazioni di rischio on-line tramite:

- La presentazione ai Consigli di Classe e al Consiglio d'Istituto della E-safety Policy qui prodotta e la sua diffusione a tutti i genitori
- La diffusione di tutto il materiale informativo ricevuto e reperito sul tema
- La presentazione del portale www.generazioniconnesse.it e l'invito a consultarlo da parte di genitori e ragazzi
- L'organizzazione di incontri con esperti aperti a genitori, docenti e alunni
- L'inserimento nel Patto di Corresponsabilità di un riferimento all'utilizzo consapevole delle TIC e della Rete.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2019/2020)

- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.

- Effettuare un’analisi del fabbisogno formativo del corpo docente sull’utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Coinvolgere una rappresentanza dei genitori per individuare i temi di maggiore interesse nell’ambito dell’educazione alla cittadinanza digitale.

AZIONI (da sviluppare nell’arco dei tre anni scolastici successivi)

Scegliere almeno 1 di queste azioni

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

Capitolo 3 - Gestione dell'infrastruttura e della strumentazione ICT della e nella scuola

3.1 - Protezione dei dati personali

"Le scuole sono chiamate ogni giorno ad affrontare la sfida più difficile, quella di educare le nuove generazioni non solo alla conoscenza di nozioni basilari e alla trasmissione del sapere, ma soprattutto al rispetto dei valori fondanti di una società. Nell'era di Internet e in presenza di nuove forme di comunicazione questo compito diventa ancora più cruciale. È importante riaffermare quotidianamente, anche in ambito scolastico, quei principi di civiltà, come la riservatezza e la dignità della persona, che devono sempre essere al centro della formazione di ogni cittadino".

(cfr. http://www.garanteprivacy.it/scuola).

Ogni giorno a scuola vengono trattati numerosi dati personali sugli studenti e sulle loro famiglie. Talvolta, tali dati possono riguardare informazioni sensibili, come problemi sanitari o particolari disagi sociali. Il "corretto trattamento dei dati personali" a scuola è condizione necessaria per il rispetto della dignità delle persone, della loro identità e del loro diritto alla riservatezza. Per questo è importante che le istituzioni scolastiche, durante lo svolgimento dei loro compiti, rispettino la privacy, tutelando i dati personali dei soggetti coinvolti, in particolar modo quando questi sono minorenni.

La protezione dei dati personali è un diritto fondamentale dell'individuo ai sensi della Carta dei diritti fondamentali dell'Unione europea (art. 8), tutelato dal Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 (relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati).

Anche le scuole, quindi, hanno oggi l'obbligo di adeguarsi al cosiddetto GDPR (General Data Protection Regulation) e al D.Lgs. 10 agosto 2018, n. 101, entrato in vigore lo scorso 19 settembre.

In questo paragrafo dell'ePolicy affrontiamo tale problematica, con particolare riferimento all'uso delle tecnologie digitali, e indichiamo le misure che la scuola intende attuare per garantire la tutela della privacy e il diritto alla riservatezza di tutti i soggetti coinvolti nel processo educativo, con particolare attenzione ai minori. A tal fine, l'Istituto allega alla presente ePolicy i modelli di liberatoria da utilizzare e conformi alla normativa vigente, in materia di protezione dei dati

personali.

La diffusione sempre maggiore di smartphone tra i giovanissimi, l'uso di tablet a scopo didattico, la condivisione online di contenuti didattici, l'uso del registro elettronico, l'eventualità di gruppi whatsapp tra studenti/esse, genitori, docenti o tra insegnanti e studenti/esse, 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. La velocità, l'immediatezza con cui si risponde ai messaggi o si condividono foto o video, può far perdere il controllo di dati personali e mettere a rischio la reputazione e la sicurezza dei soggetti coinvolti.

Sono dati personali le informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, etc.

Fra questi, particolarmente importanti sono:

- i dati che permettono l'identificazione diretta di una persona, come i dati anagrafici (ad es. nome e cognome);
- i dati che permettono l'identificazione indiretta, come un numero di identificazione (ad es. il codice fiscale, l'indirizzo IP, il numero di targa);
- i dati rientranti in particolari categorie: si tratta dei dati cosiddetti sensibili, cioè quelli che rivelano l'origine razziale o etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, dati relativi alla salute o alla vita sessuale di una persona. Il Regolamento (UE) 2016/679 (articolo 9) ha incluso nella nozione anche i dati genetici, i dati biometrici e quelli relativi all'orientamento sessuale.

Le istituzioni scolastiche pubbliche possono trattare solamente i dati personali necessari al perseguimento di specifiche finalità istituzionali, oppure quelli espressamente previsti dalla normativa di settore. Per tali trattamenti non sono tenute a chiedere il consenso degli/lle studenti/esse.

Alcune categorie di dati personali degli/lle studenti/esse e delle famiglie, come quelli sensibili e giudiziari, devono essere trattate con estrema cautela, nel rispetto di specifiche norme di legge, verificando in primis non solo la pertinenza e completezza dei dati, ma anche la loro indispensabilità rispetto alle "finalità di rilevante interesse pubblico" che si intendono perseguire.

La scuola comunica (tramite apposita informativa) agli interessati le caratteristiche e le modalità del trattamento dei loro dati, indicando i responsabili del trattamento. Gli interessati non sono solo gli/le studenti/esse, ma anche le famiglie e gli stessi professori. Inoltre, la scuola verifica i loro trattamenti, controllando se i dati siano eccedenti rispetto alle finalità perseguite.

L'Istituto comprensivo "Minzele-Parini" tutela la privacy dei propri iscritti e si impegna a proteggere i dati personali che gli stessi comunicano. La raccolta ed il trattamento dei dati personali avvengono, quando necessari, in relazione all'esecuzione dei servizi richiesti dall'utente, o quando l'utente stesso decide di comunicare i propri dati personali. In questo caso, l'Istituto informa l'utente sulle

finalità della raccolta al momento della stessa e, ove necessario, richiede il consenso all'utente.
Inoltre:

- il personale non deve condividere numeri di telefono personali o indirizzi di posta elettronica privati con la componente studentesca e con i genitori.
- le fotografie o i video da pubblicare sul sito che includano allieve e allievi saranno selezionati con cura e non permetteranno a singoli di essere chiaramente identificati a meno che non si tratti di eventi particolari per cui le famiglie potranno concedere opportuna autorizzazione. La scuola cercherà di utilizzare fotografie o video di gruppo piuttosto che foto integrali di singoli.
- i nomi completi di alunne e alunni saranno evitati sul sito web in particolare se in associazione con le loro fotografie.

3.2 - Accesso ad Internet

1. *L'accesso a Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale.*
2. *Ogni persona ha eguale diritto di accedere a Internet in condizioni di parità, con modalità tecnologicamente adeguate e aggiornate che rimuovano ogni ostacolo di ordine economico e sociale.*
3. *Il diritto fondamentale di accesso a Internet deve essere assicurato nei suoi presupposti sostanziali e non solo come possibilità di collegamento alla Rete.*
4. *L'accesso comprende la libertà di scelta per quanto riguarda dispositivi, sistemi operativi e applicazioni anche distribuite.*
5. *Le Istituzioni pubbliche garantiscono i necessari interventi per il superamento di ogni forma di divario digitale tra cui quelli determinati dal genere, dalle condizioni economiche oltre che da situazioni di vulnerabilità personale e disabilità.*

Così recita l'art. 2 della Dichiarazione dei diritti di Internet, elaborata dalla Commissione per i diritti e i doveri in Internet, commissione costituita il 27 ottobre 2014 presso la Camera dei Deputati dalla presidente Laura Boldrini e presieduta da Stefano Rodotà. Inoltre, il 30 aprile 2016 era entrato in vigore il Regolamento UE del Parlamento Europeo e del Consiglio del 25 novembre 2015, che stabilisce le "misure riguardanti l'accesso a un'Internet aperto e che modifica la direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica e il regolamento (UE) n. 531/2012 relativo al roaming sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione".

Il diritto di accesso a Internet è dunque presente nell'ordinamento italiano ed europeo e la scuola dovrebbe essere il luogo dove tale diritto è garantito, anche per quegli studenti che non dispongono della Rete a casa. In modo coerente il PNSD (Piano Nazionale Scuola Digitale) ha tra gli obiettivi quello di "fornire a tutte le scuole le condizioni per l'accesso alla società dell'informazione e fare in modo che il "diritto a Internet" diventi una realtà, a partire dalla scuola".

Questo perché le tecnologie da un lato contribuiscono a creare un ambiente che può rendere la scuola aperta, flessibile e inclusiva, dall'altro le consentono di adeguarsi ai cambiamenti della società e del mercato del lavoro, puntando a sviluppare una cultura digitale diffusa che deve iniziare proprio a scuola.

La scuola deve dunque considerare l'ambiente online alla stregua dell'ambiente fisico e valutarne tutti gli aspetti legati alla sicurezza nel momento in cui permette a studenti/esse e docenti l'accesso alla rete tramite i dispositivi della scuola, tramite la rete scolastica o tramite i dispositivi personali.

In riferimento alla security non è sufficiente prestare attenzione all'infrastruttura hardware e alla rete (wireless e non), ma è necessario considerare anche la sicurezza di tutti gli aspetti che riguardano la gestione degli account degli utenti (in modo differenziato tra studenti, insegnanti e personale amministrativo), il filtraggio dei contenuti (possibilmente in modo differenziato in base all'età) e gli aspetti legali in relazione prevalentemente alla privacy.

Nel nostro istituto ogni docente è responsabile delle proprie credenziali di accesso al registro elettronico e all'account di Istituto. In caso di smarrimento o dimenticanza i docenti o il personale ATA possono rivolgersi alla segreteria e far presente il problema.

L'IC "Minzele-Parini" dispone dell'accesso alla rete wi-fi in gran parte delle aule dei plessi appartenenti all'Istituto Comprensivo. La rete non possiede filtri particolari di protezione.

Per questo la scuola deve prendere tutte le necessarie precauzioni per evitare l'accesso online da parte di studenti e studentesse, a materiali non adatti a loro all'interno della scuola. Questo può avvenire attraverso l'adozione di sistemi di filtraggio software e hardware o attraverso Internet provider che forniscono un servizio ad hoc. Le esigenze possono variare in base all'età degli studenti e delle studentesse ed è possibile differenziare l'accesso (come spesso avviene tra studenti e docenti), ma le indicazioni sono di permettere un utilizzo adeguato delle risorse web per creare un ambiente sicuro, simile a quello "reale" e che permetta agli studenti, fin da piccoli, di affrontare il web con la guida degli insegnanti.

L'obiettivo principale resta quello di arricchire ed ampliare le attività didattiche, secondo quanto prevede il curricolo scolastico, l'età e la maturità degli/lle studenti/esse.

Per la realizzazione di un ambiente sicuro, l'accesso a
Internet è consentito al personale docente e non docente solo ad esclusivo uso didattico e amministrativo. Gli alunni possono utilizzare, solo per uso didattico, la rete sotto la diretta responsabilità di un insegnante.

3.3 - Strumenti di comunicazione online

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

Sito web della scuola

Il nostro Istituto possiede un sito istituzionale, che è gestito da un provider esterno e che viene costantemente aggiornato e arricchito con le attività svolte e le news dall'Animatore Digitale dopo che il Dirigente scolastico ne valuta la sicurezza e l'adeguatezza sotto i diversi profili dell'accessibilità, della pertinenza dei contenuti, del rispetto della privacy, ecc.
Esso offre al proprio interno i seguenti servizi alle famiglie ed agli utenti esterni:

- consultazione elenchi libri di testo;
- piano dell'offerta formativa;
- regolamento d'Istituto;
- informazioni generali sull'Istituto;
- informazioni sui progetti attivati dall'Istituto;
- informazioni sull'amministrazione dell'Istituto;
- avvisi e comunicazioni;
- moduli vari;
- accesso diretto al Registro Elettronico;
- accesso al progetto Generazioni Connesse.

Registro elettronico

Ogni famiglia ha ricevuto le credenziali per l'accesso riservato al registro elettronico a seguito dell'emergenza COVID-19 per l'avvio della didattica a distanza. L'uso del registro elettronico, al momento, è limitato a consentire l'accesso alla piattaforma Collabora, utilizzata per l'erogazione delle lezioni a distanza. La famiglie non hanno ancora accesso alla visualizzazione di assenze, valutazioni, note e osservazioni.

E-mail

L'account di posta elettronica è solo quello istituzionale utilizzato ordinariamente dagli uffici amministrativi, sia per la posta in ingresso che in uscita. L'eventuale invio o ricevimento di posta a scopi didattici avverrebbe solo su autorizzazione del Dirigente scolastico e operativamente sarebbe svolto dall'assistente amministrativo addetto. La posta elettronica è protetta da antivirus, e quella certificata anche dall'antispam.

In riferimento all'uso degli strumenti di comunicazione online per la circolazione di informazioni e comunicazioni interne, come avviene generalmente fra i docenti mediante ad esempio l'uso di gruppi whatsapp o telegram, è importante ricordare quello che si può definire "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 norme vigenti nella nostra scuola, come da Contratto Integrativo di Istituto (2019/2020), sono le seguenti:

- Le comunicazioni di servizio (avvisi, circolari, ecc.) vengono pubblicate sul sito istituzionale entro le ore 19.00, con la stessa tempistica le comunicazioni sono inoltrate al personale tramite la posta elettronica di servizio o altra posta elettronica comunicata e autorizzata all'uso dal personale stesso o altre piattaforme (gruppo Whatsapp Docenti);
- Per esigenze di sevizio è consentito inviare comunicazioni al personale mediante e-mail dalle ore 08:00 alle ore 13:30 e dalle ore 15:00 alle ore 19:00 esclusi festivi e prefestivi. Tale modalità di comunicazione è aggiuntiva e non sostitutiva rispetto alla comunicazione sul sito istituzionale, fatta eccezione per le comunicazioni individuali e di natura riservata.

È importante sottolineare però che per le chat informali fra colleghi, o fra docenti e genitori, non esiste una vera e propria regolamentazione, e per tale ragione è fondamentale, a partire dal buon senso e da una riflessione sulle peculiarità del mezzo, che si elaborino regole condivise sull'uso delle stesse.

- Mettere in chiaro fin dall'inizio, comprendere e rispettare sempre le finalità del gruppo, scrivendo e pubblicando solo contenuti pertinenti a tali finalità;
- Usare sempre un linguaggio adeguato e il più possibile chiaro e preciso (come già sottolineato la comunicazione online si presta spesso a non pochi fraintendimenti);
- Evitare discussioni di questioni che coinvolgono due o pochi interlocutori, onde evitare di annoiare e disturbare gli altri componenti del gruppo;
- Non condividere file multimediali troppo pesanti;
- Evitare il più possibile di condividere foto di studenti in chat;
- Indirizzare solo domande precise e chiare, a cui si possano dare risposte altrettanto brevi e precise;
- Evitare messaggi troppo spezzettati, cercando il più possibile di essere brevi ed esaustivi allo stesso tempo.

3.4 - Strumentazione personale

I dispositivi tecnologici sono parte integrante della vita personale di ciascuno, compresa quella degli/lle studenti/esse e dei docenti (oltre che di tutte le figure professionali che a vario titolo sono inseriti nel mondo della scuola), ed influenzano necessariamente anche la didattica e gli stili di apprendimento. Comprendere il loro utilizzo e le loro potenzialità innovative, diventa di cruciale importanza, anche considerando il quadro di indirizzo normativo esistente e le azioni programmatiche, fra queste il Progetto Generazioni Connesse e il più ampio PNSD.

La presente ***ePolicy*** contiene indicazioni, revisioni o eventuali integrazioni di Regolamenti già esistenti che disciplinano l'uso dei dispositivi personali in classe, a seconda dei vari usi, anche in considerazione dei dieci punti del Miur per l'uso dei dispositivi mobili a scuola (BYOD, "Bring your own device").

Risulta fondamentale per la comunità scolastica aprire un dialogo su questa tematica e riflettere sulle possibilità per l'Istituto di dotarsi di una regolamentazione condivisa e specifica che tratti tali aspetti, considerando aspetti positivi ed eventuali criticità nella e per la didattica.

Per gli studenti della Scuola primaria e Secondaria : è vietato l'utilizzo di cellulari per l'intera durata delle attività scolastiche. È consentito agli alunni con Bisogni Educativi Speciali utilizzare il proprio notebook o tablet. È consentito a tutti gli studenti, in casi concordati con il docente (uscite didattiche, produzioni multimediali, uso di piattaforme didattiche come Edmodo, Weschool, Collabora; Nearpod, ecc) l'utilizzo di dispostivi elettronici personali per scopi didattici. Nel caso in cui gli alunni debbano comunicare con la famiglia durante l'orario scolastico possono utilizzare la linea fissa della scuola chiedendo ad un collaboratore; allo stesso modo le famiglie devono chiamare al numero telefonico della scuola se hanno assoluta necessità di parlare con i figli.

Per i docenti: durante il loro orario di servizio è consentito l'utilizzo di dispostivi elettronici personali solo ed esclusivamente per fini educativo-didattici.

Per il personale della scuola: è consentito l'utilizzo di dispostivi elettronici personali solo ed esclusivamente per esigenze di servizio.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2019/2020).

- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

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

- Organizzare uno o più eventi o attività volti a formare i genitori dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

Capitolo 4 - Rischi on line: conoscere, prevenire e rilevare

4.1 - Sensibilizzazione e Prevenzione

Il rischio online si configura come la possibilità per il minore di:

- commettere azioni online che possano danneggiare se stessi o altri;
- essere una vittima di queste azioni;
- osservare altri commettere queste azioni.

È importante riconoscere questi fenomeni e saperli distinguere tra loro in modo da poter poi adottare le strategie migliori per arginarli e contenerli, ma è altrettanto importante sapere quali sono le possibili strategie da mettere in campo per ridurre la possibilità che questi fenomeni avvengano. Ciò è possibile lavorando su aspetti di ampio raggio che possano permettere una riduzione dei fattori di rischio e di conseguenza una minore probabilità che i ragazzi si trovino in situazioni non piacevoli. È importante che abbiano gli strumenti idonei per riconoscere possibili situazioni di rischio e segnalarle ad un adulto di riferimento.

Gli strumenti da adottare per poter ridurre l'incidenza di situazioni di rischio si configurano come interventi di **sensibilizzazione e prevenzione.**

- Nel caso della **sensibilizzazione** *si tratta di azioni che hanno come obiettivo quello di innescare e promuovere un cambiamento; l'intervento dovrebbe fornire non solo le informazioni necessarie (utili a conoscere il fenomeno), ma anche illustrare le possibili soluzioni o i comportamenti da adottare.*
- Nel caso della **prevenzione** *si tratta di un insieme di attività, azioni ed interventi attuati con il fine prioritario di promuovere le competenze digitali ed evitare l'insorgenza di rischi legati all'utilizzo del digitale e quindi ridurre i rischi per la sicurezza di bambine/i e ragazze/i.*

Le misure di sensibilizzazione e di prevenzione comprendono l'integrazione nel curricolo dei temi legati al corretto utilizzo delle TIC e di Internet: la progettazione di unità didattiche specifiche deve essere pianificata a livello di dipartimenti disciplinari, garantendo un intervento su ogni classe. La scuola si avvale della collaborazione di enti e associazioni per realizzare incontri rivolti alla componente studentesca e alle famiglie con l'intento di fornire ogni elemento utile alla prevenzione e alla gestione dei problemi relativi alla sicurezza informatica; le famiglie sono invitate a proporre tematiche di particolare interesse su cui la scuola focalizzerà il proprio intervento.

Gli interventi di **sensibilizzazione** hanno come obiettivo quello di innescare e promuovere un

cambiamento, ma per far sì che un intervento di sensibilizzazione sia efficace, è quindi importante fornire ai beneficiari informazioni chiare su quello che è lo stato attuale del tema che vogliamo trattare e illustrare le possibili soluzioni o comportamenti da adottare per indurre l'intera comunità al cambiamento.

Per quanto riguarda gli interventi di prevenzione, invece, è necessario distinguere tre distinti livelli:

- **Prevenzione Universale.** Un programma di questo tipo parte dal presupposto che tutti gli studenti siano potenzialmente a rischio. Si tratta quindi di interventi diretti al grande pubblico o a un intero gruppo di una popolazione che non è stato identificato sulla base del rischio individuale. Questi interventi possono produrre cambiamenti in grandi popolazioni (ad es. si pensi ad un programma dedicato alle competenze emotive, oppure alla cittadinanza digitale o, ancora, a interventi con esperti sui rischi connessi all'uso delle tecnologie e di Internet).
- **Prevenzione Selettiva.** Un programma dedicato ad un gruppo di studenti in cui il rischio online è presente. In questo caso la presenza del rischio è stata individuata tramite precedenti indagini, segnalazioni fatte dalla scuola, oppure dalla conoscenza della presenza di fattori di rischio in quel determinato territorio. In questi casi gli interventi sono mirati e prevedono programmi formativi strutturati che hanno l'obiettivo di migliorare le competenze digitali e le strategie di problem solving. Può essere un valido programma se si osservano casi in cui la prevenzione universale non ha dato gli esiti previsti. Questo genere di intervento viene adottato dall'intero Consiglio di classe, che interviente trasversalmente sul tema specifico.
- **Prevenzione Indicata.** Un programma di intervento sul caso specifico, è quindi pensato e strutturato per adattarsi agli/lle studenti/studentesse con l'obiettivo di ridurre i comportamenti problematici, oppure dare supporto alle vittime. Per la sua natura questo tipo di intervento si avvale di professionalità diverse perché spesso affronta problemi legati alla salute mentale del minore per cui è opportuno coinvolgere anche la famiglia del/lla ragazzo/a.

Per la scuola, i programmi che possono essere realizzati con maggiore frequenza ricadono nel primo livello di Prevenzione Universale e sono sicuramente consigliati proprio perchè vanno a formare e consolidare quelle competenze educative di base necessarie a poter gestire le situazioni di vita che i/le ragazzi/e sperimentano online.

Quando un evento problematico connesso ai rischi online coinvolge il contesto scolastico, è fondamentale per la scuola poter dare una risposta il più possibile integrata, che trovi la sua espressione di indirizzo in procedure chiare di cui deve dotarsi e che includano la collaborazione (prevedendo accordi specifici) con la rete dei servizi locali (in primis le ASL e la Polizia Postale).

La responsabilità dell'azione preventiva ed educativa, infatti, chiama in campo diverse agenzie educative oltre alla scuola, come la famiglia, ma non solo (istituzioni, associazioni, società civile, etc.), ciascuna con un proprio compito nei confronti di bambini e bambine e di adolescenti.

La necessità di supportare un uso positivo e consapevole delle TIC da parte dei più giovani, sia in un'ottica di tutela dai rischi potenziali che nella valorizzazione delle opportunità esistenti, pone la

scuola e i genitori di fronte alla sfida di riconsiderare la propria identità, il proprio ruolo educativo e le proprie risorse, oltre allo stato dei rapporti reciproci per un patto educativo da rinnovare costantemente.

4.2 - Cyberbullismo: che cos'è e come prevenirlo

La legge 71/2017 "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo", nell'art. 1, comma 2, definisce il cyberbullismo:

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

La stessa legge e le relative **Linee di orientamento per la prevenzione e il contrasto del cyberbullismo** indicano al mondo scolastico ruoli, responsabilità e azioni utili a prevenire e gestire i casi di cyberbullismo. Le linee prevedono:

- formazione del personale scolastico, prevedendo la partecipazione di un proprio referente per ogni autonomia scolastica;
- sviluppo delle competenze digitali, tra gli obiettivi formativi prioritari (L.107/2015);
- promozione di un ruolo attivo degli studenti (ed ex studenti) in attività di peer education;
- previsione di misure di sostegno e rieducazione dei minori coinvolti;
- Integrazione dei regolamenti e del patto di corresponsabilità con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti;
- Il sistema scolastico deve prevedere azioni preventive ed educative e non solo sanzionatorie.
- **Nomina del Referente per le iniziative di prevenzione e contrasto che:**
    - Ha il compito di coordinare le iniziative di prevenzione e contrasto del cyberbullismo. A tal fine, può avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio.
    - Potrà svolgere un importante compito di supporto al dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d'istituto), atti e documenti (PTOF, PdM, Rav).

Il cyberbullismo ha caratteristiche proprie rispetto al bullismo tradizionale, in quanto la diffusione di materiale tramite Internet è incontrollabile e un contenuto offensivo e denigratorio online può diventare virale e distruggere in alcuni casi la reputazione della vittima. Inoltre, chi offende online resta nell'anonimanto, in quanto si nasconde dietro un nickname e il cyberbullo, che può agire in ogni momento e anche lontano dalla vittima, non ne vede in modo diretto le reazioni: ciò riduce fortemente l'empatia e il riconoscimento del danno provocato.

L'impossibilità di vedere con i propri occhi l'eventuale sofferenza e umiliazione provata dalla vittima fa sì che il tutto venga percepito come "uno scherzo" divertente a cui partecipare, di cui ridere o a cui essere indifferenti. Inoltre, il cyberbullismo non lascia segni fisici evidenti sulla vittima e si consuma in un contesto virtuale che spesso viene percepito dai ragazzi come non "reale", come un mondo ludico a sé stante.

La scuola, in questo contesto, deve innanzitutto intervenire a modificare alcune convinzioni o tendenze frequenti nell'uso della Rete sia da parte dei giovani che degli adulti:

- Percezione che online non ci siano norme sociali da rispettare: fra i giovani spesso vige la falsa convinzione secondo cui la Rete sia uno spazio virtuale lontano dalla realtà, in cui vige libertà assoluta e in cui regole e norme sociali della vita quotidiana non valgono; utile in quest'ottica è l'adozione del Manifesto della Comunicazione non ostile;
- Diffusione di responsabilità: tutti quelli che partecipano anche solo con un like o un commento diventano, di fatto, corresponsabili delle azioni del cyberbullo facendo accrescere la portata dell'azione; mettere un "like" su un social network commentare o condividere una foto o un video che prende di mira qualcuno o semplicemente tacere pur sapendo, mette ragazzi e ragazze nella condizione di avere una responsabilità.

La riflessione trasversale su questo tema, da parte dell'intera comunità scolastica, ha come obiettivo fondamentale la comprensione del fenomeno: il cyberbullismo non è una problematica che riguarda unicamente vittima e cyberbullo, ma un fenomeno sociale e di gruppo. Infatti, centrale è il ruolo delle agenzie educative e di socializzazione (formali e informali) più importanti per gli adolescenti: la famiglia, la scuola, i media, le tecnologie digitali e il gruppo dei pari.

Per questo motivo, è necessario riconoscere il fenomento immediatamente, da alcuni importanti segnali generali che può manifestare la potenziale vittima di cyberbullismo:

- Appare nervosa quando riceve un messaggio o una notifica;
- Sembra a disagio nell'andare a scuola o finge di essere malata (ha spesso mal di stomaco o mal di testa);
- Cambia comportamento ed atteggiamento in modo repentino;
- Mostra ritrosia nel dare informazioni su ciò che fa online;
- Soprattutto dopo essere stata online, mostra rabbia o si sente depressa;
- Inizia ad utilizzare sempre meno Pc e telefono (arrivando ad evitarli);
- Perde interesse per le attività familiari o per le attività extra-scolastiche che prima svolgeva;
- Il suo rendimento scolastico peggiora.

Per far sì che l'intera comunità educante prenda coscienza della gravità del fenomeno, che come abbiamo visto coinvolge molteplici attori, è importante che tutti i docenti si formino sul tema e conoscano la normativa di riferimento (Legge 71/2017), che oltre a prevedere la procedura di ammonimento per minori coinvolti in accertati episodi di cyberbullismo, definisce con precisione i reati connessi agli atti di bullismo e cyberbullismo. In particolare:

- percosse (art. 581),
- lesione personale (art. 582),
- ingiuria (art. 594),
- diffamazione (art. 595),
- violenza privata (art. 610),
- minaccia (art. 612),
- danneggiamento (art. 635).

Inoltre, le responsabilità per atti di bullismo e cyberbullismo compiute dal minorenne possono ricadere anche su:

- i genitori, perché devono educare adeguatamente e vigilare, in maniera adeguata all'età del figlio, cercando di correggerne comportamenti devianti. Questa responsabilità generale persiste anche per gli atti compiuti nei tempi di affidamento alla scuola (culpa in educando).
- gli insegnanti e la scuola: perché nei periodi in cui il minore viene affidato all'Istituzione scolastica il docente è responsabie della vigilanza sulle sue azioni e ha il dovere di impedire comportamenti dannosi verso gli altri/e ragazzi/e, insegnanti e personale scolastico o verso le strutture della scuola stessa. A pagare in primis sarà la scuola, che poi potrà rivalersi sul singolo insegnante. La responsabilità si estende anche a viaggi, gite scolastiche, manifestazioni sportive organizzate dalla scuola (culpa in vigilando).
- esiste poi una culpa in organizzando, che si ha quando la scuola non mette in atto le azioni previste per la prevenzione.

Per questo, l'IC Minzele Parini, ha da subito nominato la figura del **Referente**, che si occupa di coordinare regolarmente iniziative di prevenzione e contrasto ai fenomeni di bullismo e cyberbullismo. Tra le iniziative già intraprese, si segnalano interventi di peer education per un ruolo attivo degli studenti, in particolare sui temi della cittadinanza digitale e della comunicazione non ostile, oltre a iniziative di prevenzione universale, rivolti al personale scolastico, a studenti e studentesse e alle famiglie, in collaborazione con la Polizia Postale e con gli enti territoriali.

4.3 - Hate speech: che cos'è e come

prevenirlo

Il fenomeno di “incitamento all’odio” o “discorso d’odio”, indica discorsi (post, immagini, commenti etc.) e pratiche (non solo online) che esprimono odio e intolleranza verso un gruppo o una persona (identificate come appartenente a un gruppo o categoria) e che rischiano di provocare reazioni violente, a catena. Più ampiamente il termine “hate speech” indica un’offesa fondata su una qualsiasi discriminazione (razziale, etnica, religiosa, di genere o di orientamento sessuale, di disabilità, eccetera) ai danni di una persona o di un gruppo.

Tale fenomeno, purtroppo, è sempre più diffuso ed estremamente importante affrontarlo anche a livello educativo e scolastico con l’obiettivo di:

- fornire agli studenti gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di hate speech, in particolare legati alla razza, al genere, all’orientamento sessuale, alla disabilità;
- promuovere la partecipazione civica e l’impegno, anche attraverso i media digitali e i social network;
- favorire una presa di parola consapevole e costruttiva da parte dei giovani.

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere in relazione a questa problematica.

Si tratta di attività di analisi e di produzione mediale, finalizzate soprattutto a:

- riflettere sull'uso del linguaggio usato per comunicare e sul 'peso' delle parole che utilizziamo con gli altri, in particolare facendo riferimento al 'Manifesto della Comunicazione non ostile', sul quale è possibile lavorare in maniera trasversale in tutte le discipline, con specifiche attività didattiche proposte da Paole Ostili.
- creare un clima di collaborazione fra compagni (*cooperative learning* e *peer education*), contrastando il linguaggio dell'odio;
- implementare la metodologia didattica del debate, che consente di lavorare sulla discussione guidata da regole ben precise, per portare gli alunni ad argomentare le proprie opiniuoni rispettando quelle degli altri, in un clima collaborativo (Libertà di espressione che non diventa occasione di offesa)
- utilizzare il linguaggio mediatico come veicolo di inclusione.

4.4 - Dipendenza da Internet e gioco online

La Dipendenza da Internet fa riferimento all’utilizzo eccessivo e incontrollato di Internet che, al pari di altri comportamenti patologici/dipendenze, può causare o essere associato a isolamento sociale, sintomi da astinenza, problematiche a livello scolastico e irrefrenabile voglia di utilizzo della Rete.

L'istituto è intenzionato a promuovere azioni di prevenzione attraverso percorsi sul benessere digitale?

Anche nel caso della dipendenza da Internet, il primo passo che la scuola deve muovere va verso la conoscenza del fenomeno: la comunità scolastica, quindi, deve riconoscere tempestivamente alcune caratteristiche specifiche di questa forma di dipendenza e fornire gli strumenti agli studenti e alle studentesse affinché questi siano consapevoli dei rischi che comporta l'iperconnessione.

I segnali patologici di questo che viene descritto come "un vero e proprio abuso della tecnologia", anche denominato "Internet Addiction Disorder" (I.A.D. coniato dallo psichiatra Ivan Goldberg 1996), sono specifici così come accade per le altre dipendenze più "tradizionali". In particolare, si hanno:

- la tolleranza, ossia quando vi è un crescente bisogno di aumentare il tempo su internet;
- l'astinenza quando, cioè, vi è l'interruzione o la riduzione dell'uso della Rete che comporta ansia, agitazione psicomotoria, fantasie, pensieri ossessivi (malessere psichico e/o fisico che si manifesta quando s'interrompe o si riduce il comportamento).

Tutto questo ha ripercussioni sulla sfera delle relazioni interpersonali che diventano via via più povere e alle quali si preferisce il mondo virtuale, con alterazioni dell'umore e della percezione del tempo.

Da sottolineare, la nomofobia (nomo deriva da "no-mobile") termine usato per categorizzare quei soggetti che sperimentano emozioni negative, quali ansia, tristezza e rabbia quando non sono connessi con il proprio smartphone.

Anche in questo caso, la scuola ha la possibilità di fare formazione e di indicare strategie per un uso più consapevole delle tecnologie per favorire il **"benessere digitale"**, cioè la capacità di creare e mantenere una relazione sana con la tecnologia.

La tecnologia infatti ha modificato gli ambienti che viviamo e ha un impatto sulla qualità della vita. Gli elementi che contribuiscono al benessere digitale sono:

- la ricerca di equilibrio nelle relazioni anche online
- l'uso degli strumenti digitali per il raggiungimento di obiettivi personali
- la capacità di interagire negli ambienti digitali in modo sicuro e responsabile
- la capacità di gestire il sovraccarico informativo e le distrazioni (ad esempio, le notifiche).

La scuola, dotandosi di un curricolo digitale trasversale, si impegna ad approfondire anche i temi legati al benessere digitale. Risulta fondamentale:

- favorire innanzitutto l'integrazione della tecnologia nella didattica, mostrando un suo utilizzo funzionale che possa rendere più consapevoli i ragazzi e le ragazze delle proprie abitudini online.
- riflettere sulla tecnologia come strumento per raggiungere i propri obiettivi e non come

distrazione o addirittura ostacolo.

- Strutturare regole condivise e stipulare con loro una sorta di “patto” d’aula e, infine, proporre delle alternative metodologiche e didattiche valide che abbiano come strumento giochi virtuali d’aula, adoperando la LIM o il dispositivo personale.
- proporre periodicamente questionari per misurare il proprio modo di stare bene nella rete (utile strumento è l'opuscolo curato da R. Alborghetti, Social o Dissocial?): come trascorri il tempo on line? Quando aggiunge valore alla tua vita e quando ti fa perdere tempo? Quale atteggiamento potrei cambiare quando sono online? Che ruolo ha e deve avere la tecnologia (internet o il gioco) nella mia vita?

Se controlliamo la tecnologia possiamo usarne il pieno potenziale e trarne vantaggi.

4.5 - Sexting

Il “sexting” è fra i rischi più diffusi connessi ad un uso poco consapevole della Rete. Il termine indica un fenomeno molto frequente fra i giovanissimi che consiste nello scambio di contenuti mediali sessualmente espliciti; i/le ragazzi/e lo fanno senza essere realmente consapevoli di scambiare materiale (pedopornografico) che potrebbe arrivare in mani sbagliate e avere conseguenze impattanti emotivamente per i protagonisti delle immagini, delle foto e dei video.

Secondo una recente ricerca di Skuola.net per la Polizia di Stato - ricerca che ha coinvolto 6.500 ragazzi tra i 13 e i 18 anni - il 24% di loro ha scambiato almeno una volta immagini intime con il partner via chat o social (fenomeno conosciuto come sexting). Tra questi, il 15% ha subito la condivisione con terzi, senza consenso, di questo materiale. Il motivo più frequente, riportato dalle vittime? Un banale “scherzo” (49%), a dimostrazione di quanto possano essere sottovalutate le reali conseguenze di tale diffusione. Tra le altre motivazioni, il ricatto (11%) o la vendetta (7%): il revenge porn, pure presente, viene surclassato dalla leggerezza e dalla goliardia ma gli effetti sono drammaticamente gli stessi. La reazione più diffusa nella maggior parte dei casi è il silenzio: il 53% ha fatto finta di niente, il 31% non ha detto nulla per non essere giudicato. Il fenomeno, come si evince da questi dati, è diffusissimo e spesso associato ad una totale mancanza di consapevolezza rispetto alla gravità dell'atto, subito o agito, di diffusione e condivisione di contenuti sessualmente espliciti, che configurano veri e propri comportamenti criminalim, persseguibili penalmente, oltre a severe ripercussioni sulla vittima in termini di autostima, di credibilità, di reputazione sociale off e on line. A ciò si associano altri comportamenti a rischio, di tipo sessuale ma anche riferibili ad abuso di sostanze o di alcool.

Per questi motivi, la scuola deve portare avanti un serio intervento di prevenzione:

- Verso i genitori: informazione circa le possibilità di attivare forme di controllo parentale della navigazione.
- Verso la componente studentesca: inserimento nel curricolo di temi legati all'affettività, alla sessualità e alle differenze di genere.

In caso di segnalazioni di questo genere, se la gravità è lieve occorre in primo luogo parlarne con alunne e alunni e rispettivi genitori, ricordando loro che l'invio e la detenzione di foto che ritraggono minorenni in pose sessualmente esplicite configura il reato di distribuzione di materiale pedopornografico. In casi di rilevante gravità occorre informare tempestivamente il Dirigente Scolastico per gli adempimenti del caso.

4.6 - Adescamento online

Il ***grooming*** (dall'inglese "groom" - curare, prendersi cura) rappresenta una tecnica di manipolazione psicologica che gli adulti potenziali abusanti utilizzano per indurre i bambini/e o adolescenti a superare le resistenze emotive e instaurare una relazione intima e/o sessualizzata. Gli adulti interessati sessualmente a bambini/e e adolescenti utilizzano spesso anche gli strumenti messi a disposizione dalla Rete per entrare in contatto con loro.

I luoghi virtuali in cui si sviluppano più frequentemente tali dinamiche sono le chat, anche quelle interne ai giochi online, i social network in generale, le varie app di instant messaging (whatsapp, telegram etc.), i siti e le app di ***teen dating*** (siti di incontri per adolescenti). Un'eventuale relazione sessuale può avvenire, invece, attraverso webcam o live streaming e portare anche ad incontri dal vivo. In questi casi si parla di adescamento o grooming online.

In Italia l'adescamento si configura come reato dal 2012 (art. 609-undecies - l'adescamento di minorenni) quando è stata ratificata la Convenzione di Lanzarote (legge 172 del 1° ottobre 2012).

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere per prevenire ed affrontare la delicata problematica dell'adescamento.

La problematica dell'adescamento online (come quella del sexting) si inquadra in uno scenario più ampio di scarsa educazione emotiva, sessuale e di assenza di competenza digitale, in riferimento al modo in cui i/le ragazzi/e vivono la propria sessualità e la propria immagine online, al loro desiderio di esprimersi e affermare se stessi.

Fondamentale, quindi, è portare avanti un percorso di educazione digitale che comprenda lo sviluppo anche di capacità quali la protezione della propria privacy e la gestione dell'immagine e dell'identità online, la capacità di gestire adeguatamente le proprie relazioni online (a partire dalla consapevolezza della peculiarità del mezzo/schermo che permette a chiunque di potersi presentare molto diversamente da come realmente è).

Altrettanto importante è un'adeguata educazione all'affettività e alla sessualità.

Il miglior modo per prevenire casi di adescamento online, infatti, è accompagnare ragazze e ragazzi in un percorso di educazione (anche digitale) all'affettività e alla sessualità. Ciò aiuterebbe a renderli più sicuri emotivamente e pronti ad affrontare eventuali situazioni a rischio, imparando

innanzitutto a gestire le proprie emozioni, il rapporto con il proprio corpo e con gli altri. È molto importante, inoltre, che ragazzi e ragazze sappiano a chi rivolgersi in caso di problemi, anche quando pensano di aver fatto un errore, si vergognano o si sentono in colpa. Gli adulti coinvolti, genitori e docenti, devono essere un punto di riferimento per il minore che deve potersi fidare di loro e non sentirsi mai giudicato, ma compreso e ascoltato. Affinché ciò avvenga è necessario tenere sempre aperto un canale di comunicazione con loro sui temi dell'affettività, del digitale e perché no, della sessualità.

Ma è altrettanto importante riconoscere un eventuale caso di adescamento online, prestando attenzione a piccoli segnali che possono essere indicatori importanti, come ad esempio un cambiamento improvviso nel comportamento di un minore. A seguire, alcuni segnali e domande che potrebbero essere di aiuto:

- Il minore ha conoscenze sessuali non adeguate alla sua età?
- Un certo video o una foto circolano online o il minore ha ricevuto o filmato, ma c'è imbarazzo e preoccupazione nel raccontare di più.
- Il minore si isola totalmente e sembra preso solo da una relazione online?
- Ci sono prese in giro e allusioni sessuali verso un bambino/ragazzo in particolare?

Una volta accertato il caso, è importante, innanzitutto, che l'adulto di riferimento non si sostituisca al minore nel rispondere, ad esempio, all'adescatore. È importante che il computer o altri dispositivi elettronici del minore vittima non vengano usati per non compromettere eventuali prove.
Casi di adescamento online richiedono l'intervento della Polizia Postale e delle Comunicazioni a cui bisogna rivolgersi il prima possibile, tenendo traccia degli scambi fra il minore e l'adescatore (ad esempio, salvando le conversazioni attraverso screenshot, memorizzando eventuali immagini o video…).
L'adescamento, inoltre, può essere una problematica molto delicata da gestire e può avere ripercussioni psicologiche significative sul minore. Per questo potrebbe essere necessario rivolgersi ad un Servizio territoriale (es. Consultorio Familiare, Servizio di Neuropsichiatria Infantile, ecc.) in grado di fornire alla vittima anche un adeguato supporto di tipo psicologico o psichiatrico.

4.7 - Pedopornografia

La pedopornografia online è un reato (art. 600-ter comma 3 del c.p.) che consiste nel produrre, divulgare, diffondere e pubblicizzare, anche per via telematica, immagini o video ritraenti bambini/e, ragazzi/e coinvolti/e in comportamenti sessualmente espliciti, **concrete o simulate** o qualsiasi rappresentazione degli organi sessuali a fini soprattutto sessuali.

La legge n. 269 del 3 agosto 1998 *"Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di schiavitù", introduce nuove fattispecie di reato (come ad esempio il turismo sessuale) e, insieme alle successive modifiche e integrazioni contenute nella* ***legge n. 38 del 6 febbraio 2006*** *"Disposizioni in materia di lotta*

contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet", segna una tappa fondamentale nella definizione e predisposizione di strumenti utili a contrastare i fenomeni di sfruttamento sessuale a danno di minori. Quest'ultima, introduce, tra le altre cose, il reato di "pornografia minorile virtuale" (artt. 600 ter e 600 quater c.p.) che si verifica quando il materiale pedopornografico rappresenta immagini relative a bambini/e ed adolescenti, realizzate con tecniche di elaborazione grafica non associate, in tutto o in parte, a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali.

Secondo la Legge 172/2012 - *Ratifica della Convenzione di Lanzarote (Art 4.) per pornografia minorile si intende ogni rappresentazione, con qualunque mezzo, di un minore degli anni diciotto coinvolto in attività sessuali esplicite, reali o simulate, o qualunque rappresentazione degli organi sessuali di un minore di anni diciotto per scopi sessuali.*

In un'ottica di attività preventive, il tema della pedopornografia è estremamente delicato, occorre parlarne sempre in considerazione della maturità, della fascia d'età e selezionando il tipo di informazioni che si possono condividere.

La pedopornografia è tuttavia un fenomeno di cui si deve sapere di più, ed è utile parlarne, in particolare se si vogliono chiarire alcuni aspetti legati alle conseguenze impreviste del sexting.

Inoltre, è auspicabile che possa rientrare nei temi di un'attività di sensibilizzazione rivolta ai genitori e al personale scolastico promuovendo i servizi di Generazioni Connesse: qualora navigando in Rete si incontri materiale pedopornografico è opportuno segnalarlo, anche anonimamente, attraverso il sito www.generazioniconnesse.it alla sezione **"Segnala contenuti illegali"** (Hotline).

Il servizio Hotline si occupa di raccogliere e dare corso a segnalazioni, inoltrate anche in forma anonima, relative a contenuti pedopornografici e altri contenuti illegali/dannosi diffusi attraverso la Rete. I due servizi messi a disposizione dal Safer Internet Centre sono il "Clicca e Segnala" di Telefono Azzurro e "STOP-IT" di Save the Children.

Una volta ricevuta la segnalazione, gli operatori procederanno a coinvolgere le autorità competenti in materia. L'intento è quello di facilitare il processo di rimozione del materiale stesso dalla Rete e allo stesso tempo consentire le opportune attività investigative finalizzate ad identificare chi possiede quel materiale, chi lo diffonde e chi lo produce, ma, soprattutto e primariamente, ad identificare i minori abusati presenti nelle immagini e video, assicurando la fine di un abuso che potrebbe essere ancora in corso e il supporto necessario.

Parallelamente, se si ravvisa un rischio per il benessere psicofisico dei/lle bambini/e, ragazzi/e coinvolte nella visione di questi contenuti sarà opportuno ricorrere a un supporto psicologico anche passando per una consultazione presso il medico di base o pediatra di riferimento. Le strutture pubbliche a cui rivolgersi sono i servizi socio-sanitari del territorio di appartenenza: Consultori Familiari, Servizi di Neuropsichiatria infantile, centri specializzati sull'abuso e il maltrattamento all'infanzia, etc.

Se si è a conoscenza di tale tipologia di reato è possibile far riferimento alla: Polizia di Stato – Compartimento di Polizia postale e delle Comunicazioni; Polizia di Stato – Questura o

Commissariato di P.S. del territorio di competenza; Arma dei Carabinieri – Comando Provinciale o Stazione del territorio di competenza; Polizia di Stato – Commissariato online.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2019/2020).

□ Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti agli/lle studenti/studentesse, con il coinvolgimento di esperti.

□ Organizzare uno o più incontri di formazione all'utilizzo sicuro e consapevole di Internet e delle tecnologie digitali integrando lo svolgimento della didattica e assicurando la partecipazione attiva degli studenti/studentesse.

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

□ Promuovere incontri e laboratori per studenti e studentesse dedicati all' Educazione Civica Digitale.

□ Organizzare uno o più incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/lle studenti/studentesse.

□ Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/lle studenti/studentesse.

Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

Il personale docente del nostro Istituto quando ha il sospetto o la certezza che uno/a studente/essa possa essere vittima o responsabile di una situazione di cyberbullismo, sexting o adescamento online ha a disposizione procedure definite e può fare riferimento a tutta la comunità scolastica.

Questa sezione dell'ePolicy contiene le procedure standardizzate per la segnalazione e gestione dei problemi connessi a comportamenti online a rischio di studenti e studentesse (vedi allegati a seguire).

Tali procedure dovranno essere una guida costante per il personale della scuola nell'identificazione di una situazione online a rischio, così da definire le modalità di presa in carico da parte della scuola e l'intervento migliore da mettere in atto per aiutare studenti/esse in difficoltà. Esse, inoltre, forniscono valide indicazioni anche per i professionisti e le organizzazioni esterne che operano con la scuola (vedi paragrafo 1.3. dell'ePolicy).

Nelle procedure:

- sono indicate le **figure preposte all'accoglienza della segnalazione e alla presa in carico e gestione del caso**.
- le modalità di coinvolgimento del referente per il contrasto del bullismo e del cyberbullismo, oltre al Dirigente Scolastico.

Inoltre, la scuola **individua le figure che costituiranno un team** preposto alla gestione della segnalazione (gestione interna alla scuola, invio ai soggetti competenti).

Nell'affrontare i casi prevediamo la **collaborazione con altre figure, enti, istituzioni e servizi presenti sul territorio** (che verranno richiamati più avanti), qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.

Tali procedure sono comunicate e condivise con l'intera comunità scolastica.

Questo risulta importante sia per facilitare l'emersione di situazioni a rischio, e la conseguente presa in carico e gestione, sia per dare un messaggio chiaro a studenti e studentesse, alle famiglie e a tutti coloro che vivono la scuola che la stessa è un luogo sicuro, attento al benessere di chi lo vive, in cui le problematiche non vengono ignorate ma gestite con una mobilitazione attenta di tutta la comunità.

La condivisione avverrà attraverso assemblee scolastiche che coinvolgono i genitori, gli studenti e le studentesse e il personale della scuola, con l'utilizzo di locandine da affiggere a scuola, attraverso news nel sito della scuola e durante i collegi docenti e attraverso tutti i canali maggiormente utili ad un'efficace comunicazione.

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

- **Cyberbullismo**: è necessario capire se si tratta effettivamente di cyberbullismo o di altra problematica. Oltre al contesto, vanno considerate le modalità attraverso le quali il comportamento si manifesta (alla presenza di un "pubblico"? Tra coetanei? In modo ripetuto e intenzionale? C'è un danno percepito alla vittima? etc.). È necessario poi valutare l'eventuale stato di disagio vissuto dagli/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 la rimozione del materiale, per quanto possibile, se online e il blocco della sua diffusione via dispositivi mobili.

Per quanto riguarda la necessità di segnalazione e rimozione di contenuti online lesivi, ciascun minore ultraquattordicenne (o i suoi genitori o chi esercita la responsabilità del minore) che sia stato vittima di cyberbullismo può inoltrare al titolare del trattamento o al gestore del sito internet o del social media un'istanza per l'oscuramento, la rimozione o il blocco dei contenuti diffusi nella Rete. Se entro 24 ore il gestore non avrà provveduto, l'interessato può rivolgere analoga richiesta al Garante per la protezione dei dati personali, che rimuoverà i contenuti entro 48 ore.

Vi suggeriamo, inoltre, i seguenti servizi:

- Servizio di Helpline 19696 e Chat di Telefono Azzurro per supporto ed emergenze;

- Clicca e segnala di Telefono Azzurro e STOP-IT di Save the Children Italia per segnalare la presenza di materiale pedopornografico online.

Si considerano da segnalare tutte quelle situazioni caratterizzate da volontarie e ripetute aggressioni mirate a insultare, minacciare, diffamare e/o ferire una persona (o un piccolo gruppo) tramite un utilizzo irresponsabile di internet. La scuola, quindi, avrà cura di porre attenzione alla rilevazione di rischi connessi alla navigazione sul web. In modo particolare al cyberbullismo,

all'adescamento online e al sexting.
In particolare si segnaleranno:

- contenuti afferenti la violazione della privacy (foto personali, l'indirizzo di casa o il telefono, informazioni private proprie o di amici, foto o video pubblicati contro la propria volontà, di eventi privati, ecc.);
- contenuti afferenti all'aggressività o alla violenza (messaggi minacciosi, commenti offensivi, pettegolezzi, informazioni false, foto o video imbarazzanti, virus, contenuti razzisti, che inneggiano
- al suicidio, immagini o video umilianti, insulti, videogiochi pensati per un pubblico adulto, ecc.);
- contenuti afferenti alla sessualità: messaggi molesti, conversazioni (testo o voce) che connotano una relazione intima e/o sessualizzata, foto o video personali con nudità o abbigliamento succinto, immagini pornografiche, foto e video in cui persone di minore età sono coinvolte o assistono ad attività sessuali (pedopornografia), ecc.

Tutte le segnalazioni riportate dal personale docente e non docente, dalle famiglie e dagli studenti/esse, verranno registrate su apposita scheda allegata.

5.2. - Come segnalare: quali strumenti e a chi

L'insegnante riveste la qualifica di pubblico ufficiale in quanto l'esercizio delle sue funzioni non è circoscritto all'ambito dell'apprendimento, ossia alla sola preparazione e tenuta delle lezioni, alla verifica/valutazione dei contenuti appresi dagli studenti e dalle studentesse, ma si estende a tutte le altre attività educative.

Le situazioni problematiche in relazione all'uso delle tecnologie digitali dovrebbero essere sempre gestite anche a livello di gruppo.

Come descritto nelle procedure di questa sezione, si potrebbero palesare due casi:

- CASO A (SOSPETTO) – Il docente ha il sospetto che stia avvenendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.
- CASO B (EVIDENZA) – Il docente ha evidenza certa che stia accadendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.

Per tutti i dettagli fate riferimento agli allegati con le procedure.

Strumenti a disposizione di studenti/esse

Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola 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.

Anche studenti e studentesse, inoltre, possono rivolgersi alla Helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

La rilevazione dei casi è compito dell'intera comunità educante, secondo la sensibilità di ciascuno e la presenza in particolari momenti o contesti. Perciò è fondamentale una corretta informazione/formazione e una sensibilizzazione di tutti gli adulti coinvolti. Il personale scolastico, soprattutto nella componente docente, ma anche in quella del personale ATA, è invitato ad evitare atteggiamenti accusatori o intimidatori, in modo tale da riuscire a ricevere dai minori più fragili segnalazioni e confidenze circa situazioni problematiche vissute.

La gestione dei casi rilevati andrà differenziata a seconda della loro gravità; è in ogni caso opportuna la condivisione a livello di Consiglio di Classe/Team di Docenti di ogni episodio rilevato.

Il docente informato del caso di (cyber)bullismo, dopo aver ricostruito fatti e responsabilità in colloqui separati coi protagonisti, redige, o fa redigere agli studenti direttamente coinvolti, un modulo di segnalazione che viene protocollato, e informa:

- Coordinatore/ Docenti di Classe (Primaria)
- Referente del cyberbullismo
- Dirigente scolastico

A. Nei casi a bassa intensità (linguaggio offensivo non reiterato, litigi online, esclusione da chat, molestie, «scherzi», lievi prepotenze), dove non è necessario avvertire le Autorità:
il Coordinatore di classe convoca gli alunni coinvolti direttamente (bullo/i, vittima/e), i genitori degli stessi (d'accordo con il CdC).
B. Nei casi a media intensità (linguaggio offensivo reiterato, litigi online, esclusione da chat, molestie, «scherzi», prepotenze che coinvolgono minori di scuole diverse), dove è necessario avvertire la Polizia postale per rimuovere i contenuti dalla rete:
il Dirigente convoca gli alunni coinvolti direttamente (bullo/i, vittima/e), i genitori degli stessi

(d'accordo con il CdC) alla presenza del Coordinatore / Docenti di Classe (Primaria), del referente del cyberbullismo e/o altro docente.
C. Nei casi ad alta intensità (grave ripercussione fisica e/o psicologica: sexting, flaming, cyberstalking, outing estorto, impersonificazione), dove è necessario avvertire la Polizia postale e l'Autorità giudiziaria, occorre agire con tempestività:
il Dirigente convoca gli alunni coinvolti direttamente (bullo/i, vittima/e) e i genitori degli stessi il giorno successivo alla segnalazione (d'accordo con il CdC), alla presenza del Coordinatore / Docenti di Classe (Primaria) (che redige verbale dell'incontro da allegare al registro dei verbali e inviare al referente cyberbullismo), del referente cyberbullismo e/o altro docente.
In tutti e tre i casi (A - B - C) il Dirigente, se lo ritiene opportuno, convoca un Consiglio di classe straordinario, per stabilire gli interventi educativi e le misure delle sanzioni disciplinari; il Dirigente, in accordo con il Consiglio di Classe, informa le famiglie degli alunni coinvolti e attiva:

- gli interventi individuali: misure di supporto per la vittima;
- le sanzioni disciplinari e percorsi rieducativi per il/i (cyber)bullo/i;
- gli interventi nel gruppo classe.

5.3. - Gli attori sul territorio

Talvolta, nella gestione dei casi, può essere necessario rivolgersi **ad altre figure, enti, istituzioni e servizi presenti sul territorio** qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.

Per una mappatura degli indirizzi di tali strutture è possibile consultare il Vademecum di Generazioni Connesse "Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all'utilizzo delle tecnologie digitali da parte dei più giovani" (seconda parte, pag. 31), senza dimenticare che la Helpline di Telefono Azzurro (19696) è sempre attiva nell'offrire una guida competente ed un supporto in tale percorso.

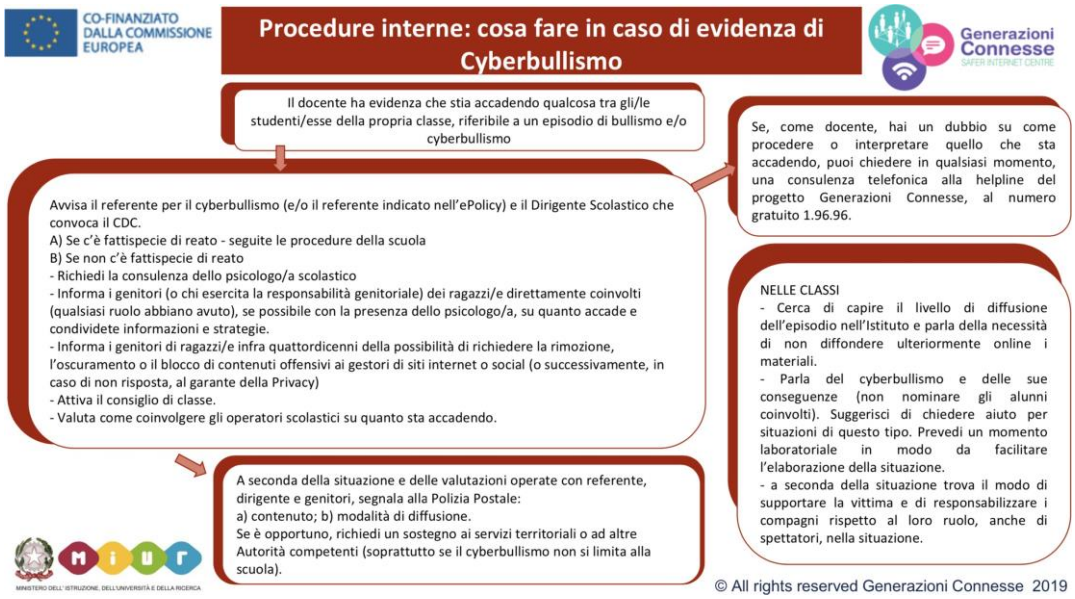
A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all'utilizzo di Internet può presentare.

- **Comitato Regionale Unicef**: laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni)**: svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare attenzione alla tutela dei minori.
- **Ufficio Scolastico Regionale**: supporta le scuole in attività di prevenzione ed anche nella segnalazione di comportamenti a rischio correlati all'uso di Internet.
- **Polizia Postale e delle Comunicazioni**: accoglie tutte le segnalazioni relative a comportamenti a rischio nell'utilizzo della Rete e che includono gli estremi del reato.

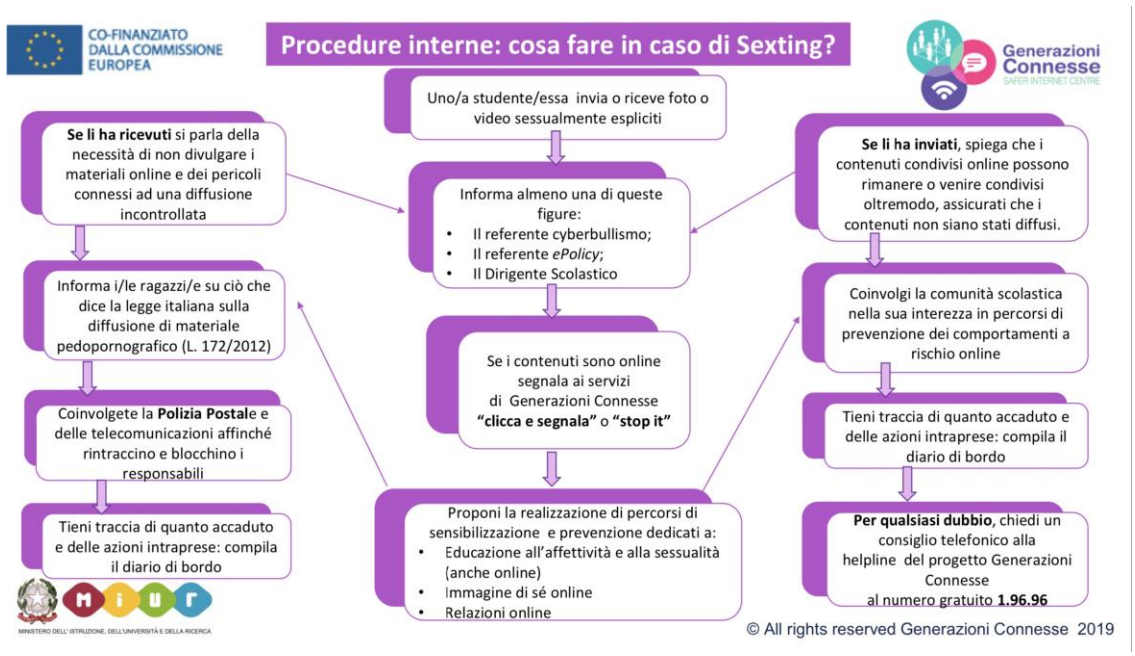
- **Aziende Sanitarie Locali**: forniscono supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in Rete. In alcune regioni, come il Lazio e la Lombardia, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da Internet e alle situazioni di rischio correlate.
- **Garante Regionale per l'Infanzia e l'Adolescenza e Difensore Civico**: segnalano all'Autorità Giudiziaria e ai Servizi Sociali competenti; accolgono le segnalazioni di presunti abusi e forniscono informazioni sulle modalità di tutela e di esercizio dei diritti dei minori vittime. Segnalano alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.
- **Tribunale per i Minorenni**: segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

5.4. - Allegati con le procedure

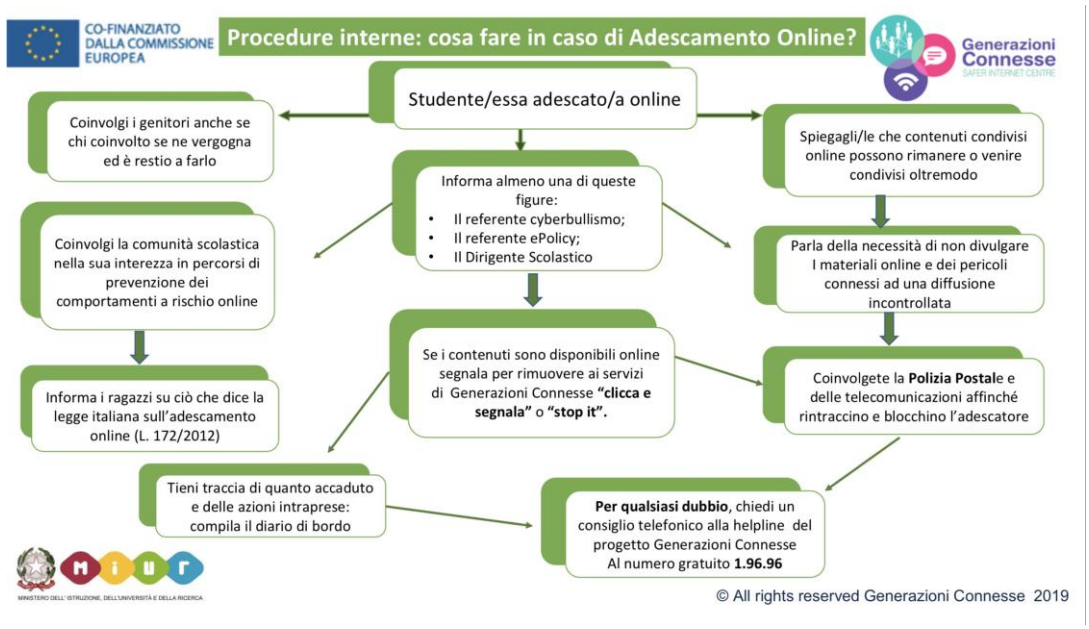
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



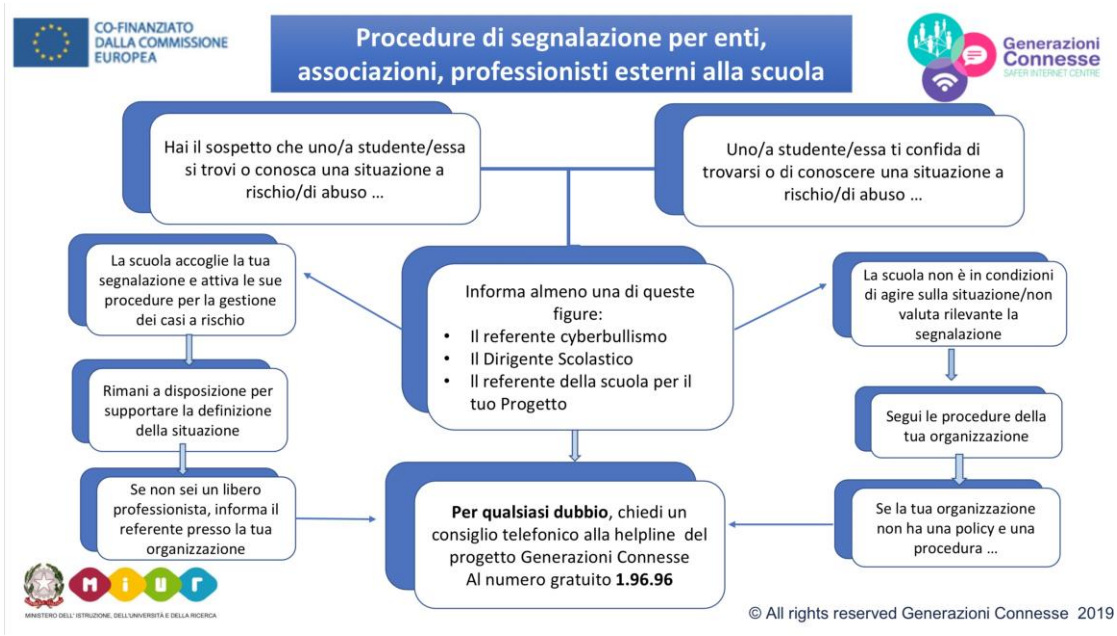
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



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



Altri allegati

- Scheda di segnalazione

- Diario di bordo
- iGloss@ 1.0 l'ABC dei comportamenti devianti online
- Elenco reati procedibili d'ufficio

Il nostro piano d'azioni

Non è prevista nessuna azione.