

Documento di ePolicy

NAIC8EN005

CASORIA IC CORTESE

VIA B. CROCE 38 - 80026 - CASORIA - NAPOLI (NA)

Prof. Luigi Storino

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 curriculum**
1. Curriculum 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.

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.

Il Dirigente Scolastico garantisce la sicurezza, anche online, di tutti i membri della comunità scolastica. Per questo motivo avrà cura di formarsi sulla sicurezza e sulla prevenzione di problematiche offline e online, in linea con il quadro normativo di riferimento e le indicazioni del MIUR; promuove la cultura della sicurezza online e collabora con il docente referente sulle tematiche del bullismo/cyberbullismo, nella definizione di corsi di formazione specifici per tutte le figure scolastiche sull' utilizzo positivo e responsabile delle TIC. Il Dirigente Scolastico ha la responsabilità di gestire ed intervenire nei casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali.

L'Animatore digitale supporta il personale scolastico da un punto di vista non solo tecnico-informatico, ma anche in riferimento ai rischi online, alla protezione e gestione dei dati personali, oltre che essere uno dei promotori di percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale"; inoltre, monitora e rileva eventuali episodi o problematiche connesse all'uso delle TIC a scuola, ed ha il compito di controllare che gli utenti autorizzati accedano alla Rete della scuola con apposita password, per scopi istituzionali e consentiti (istruzione e formazione).

Il Referente Bullismo e Cyberbullismo ha il compito di 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. Fondamentale, dunque, il suo ruolo non solo in ambito scolastico ma anche in quello extrascolastico, in quanto ha il compito di coinvolgere, con progetti e percorsi formativi ad hoc, studenti, colleghi e genitori

I Docenti hanno un ruolo centrale nel diffondere la cultura dell'uso responsabile delle TIC e della Rete. Nei diversi dipartimenti hanno integrato parti del curriculum della propria disciplina con approfondimenti ad hoc, promuovendo l'uso delle tecnologie digitali nella didattica. I docenti accompagnano e supportano 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; hanno il dovere morale e professionale di segnalare al Dirigente Scolastico qualunque problematica, violazione o abuso, anche online, che vede coinvolti studenti e studentesse.

Il personale Amministrativo, Tecnico e Ausiliario (ATA) viene coinvolto nella segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo, insieme ad altre figure e nel raccogliere, verificare e valutare le informazioni inerenti possibili casi di bullismo/cyberbullismo.

Il DSGA assicura, nei limiti delle risorse disponibili, gli interventi tecnici per garantire che l'infrastruttura tecnologica e i canali di comunicazione digitali siano funzionanti e sicuri.

I Genitori, in continuità con l'Istituto scolastico, sono invitati ad 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; sono invitati a 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. È estremamente importante che accettino e condividano quanto scritto nell'ePolicy dell'Istituto.

Gli Studenti si impegnano a comprendere e ad applicare la e-policy della scuola, nonché a segnalare abusi e usi impropri. Intraprendono le azioni attese e loro indicate se loro stessi o un compagno o una compagna sono in situazioni a rischio online. Applicano i regolamenti (quelli generali e quelli specifici delle aule di informatica) e le pratiche della scuola sulla sicurezza online.

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, saranno individuate 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.

L'Istituzione scolastica si è dotata 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. Tale documento chiarisce il sistema di azioni e le procedure di segnalazione da seguire valide anche per i professionisti e le organizzazioni esterne, finalizzate a rilevare e gestire le problematiche connesse ad un uso non consapevole delle tecnologie digitali.

In questo modo, si facilita la presa in carico da parte della scuola, qualora si verificassero problematiche derivanti da un utilizzo non corretto delle tecnologie digitali o quando, nei casi più estremi, si sospettassero forme di maltrattamento/abuso sia nel reale che nel virtuale, sia di tipo fisico che psicologico a danno di minori. Tale documento permette di tutelare ragazzi e ragazze da comportamenti potenzialmente rischiosi messi in atto da soggetti esterni alla scuola e che si trovano ad operare all'interno dell'Istituto.

In coerenza con il percorso intrapreso e con le azioni che l'Istituto già ha posto in essere, la predisposizione di un'informativa sintetica sull'ePolicy comprensiva delle procedure di segnalazione garantisce un migliore rapporto fiduciario fra scuola e famiglia, consente di distinguere i ruoli e le azioni da compiere e di attivare direttamente, a seconda della tipologia dei casi da segnalare, le autorità competenti collaborando con i servizi del territorio per la prevenzione e la gestione di quanto rilevato, in un'ottica di gestione condivisa degli interventi.

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.

Allo stesso modo le le procedure di Segnalazione sono condivise anche con i soggetti esterni, utili qualora si verificano episodi che mettano in pericolo studenti e studentesse. Tali procedure contengono i riferimenti interni alla scuola a cui rivolgersi in tali situazioni, il referente cyberbullismo, il referente del progetto, il/la coordinatore/trice di classe.

L'informativa rivolta ai soggetti esterni è così articolata

- Premessa e obiettivi dell'informativa.
- Destinatari (organizzazioni e soggetti esterni).
- Ambiti di applicazione (il progetto specifico o delle attività) e Ruoli (individuare i docenti di riferimento del progetto specifico o delle attività).
- Regolamento / Codice di comportamento.
- Procedure di segnalazione.
- Provvedimenti nel caso di:

- omessa segnalazione
- comportamenti in violazione del codice di comportamento.

Importante la condivisione e sottoscrizione nella stipula di eventuali contratti con personale e associazioni esterne: le figure professionali e le organizzazioni coinvolte in progetti, laboratori e attività dovrebbero, prenderanno visione di tutti i documenti proposti dall'Istituto e li sottoscriverebbero preliminarmente all'avvio dei programmi con gli studenti e le studentesse, in classe o fuori.

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/le 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.

Poiché la e-policy si applica a tutta la comunità scolastica, una volta approvata in via definitiva dal Collegio Docenti e dal Consiglio d'Istituto, viene condivisa con tutti i suoi membri mediante pubblicazione sul sito della scuola.

Un'adeguata formazione/informazione, oltre che mediante il presente documento, sarà garantita mediante il link al sito www.generazioniconnesse.it e nella sezione [Osservatorio Cyberbullismo](#) sul [sito della scuola](#).

Al centro saranno posti gli studenti e le studentesse, sottolineando compiti, funzioni e attività reciproche. Nello specifico si è tenuto presente che condividere e comunicare il documento agli studenti e alle studentesse è la base di partenza per un uso consapevole e maturo dei dispositivi e della tecnologia informatica; dando loro regole condivise di sicurezza circa il comportamento da tenere a scuola e nei contesti extrascolastici ed elementi per poter riconoscere e quindi prevenire comportamenti a rischio sia personali che dei/delle propri/e compagni/e.

Altrettanto importante è la condivisione del documento con il personale scolastico perché sia orientato sull'uso corretto dei dispositivi e della Rete in linea anche con il codice di comportamento dei pubblici dipendenti;

Infine, fondamentale è la condivisione del documento ai genitori sul sito istituzionale della scuola. L'accordo di utilizzo con le famiglie verrà siglato all'inizio del primo anno, all'interno del Patto Educativo di Corresponsabilità loro rilasciato. La collaborazione con esse nel perseguire la sicurezza nell'uso delle TIC sarà in seguito costantemente incoraggiata, in occasione degli incontri scuola-famiglia, collegiali, assembleari e individuali.

La scuola promuove eventi e dibattiti formativi e informativi, anche con il coinvolgimento di esperti, e attività di peer education sulla sicurezza online.

Essa mette, inoltre, in atto azioni volte a diffondere una cultura dell'inclusione, del rispetto delle differenze e a sviluppare le competenze emotive, in modo da favorire la corretta gestione del digitale come strumento relazionale.

È stata redatta 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 sono stati valutati 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.

Ciascun attore scolastico (dai docenti agli/lle studenti/esse) è stato invitato a farsi a sua volta promotore del documento.

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.

Le infrazioni alla e-safety policy da parte di studentesse e studenti possono configurarsi come infrazioni lievi, casi gravi e veri e propri reati.

Esse includono: l'uso di siti e strumenti non espressamente autorizzati dai docenti durante le lezioni o per visualizzare o scaricare materiali non consentiti; l'uso non autorizzato del cellulare durante l'orario scolastico; l'uso di social network in orario scolastico; l'invio di messaggi, foto e/o e-mail inappropriati; la violazione della privacy altrui; l'accesso a, il download e la diffusione di materiali offensivi, diffamatori, omofobici, razzisti, discriminatori e/o violenti; la produzione di riprese audio e/o video non autorizzate; la violazione dei diritti d'autore; l'invio di offese e insulti tramite messaggi di testo, e-mail o social network, l'esclusione da gruppi online (e tutti gli atti configurabili come cyberbullismo); il furto d'identità; il possesso di foto o video che riproducono situazioni violente, intime o offensive; il furto e l'uso illecito di credenziali; la frequentazione di siti pro-suicidio, pro-bulimia e/o pro-anoressia; il gioco d'azzardo online.

Per quanto concerne l'uso dei cellulari, si ricorda che, come ribadito nel Collegio del 26/10/2019, agli alunni è vietato utilizzare il telefono cellulare o altri dispositivi elettronici durante lo svolgimento delle attività didattiche (ne è consentito l'utilizzo, se previsto per lo svolgimento di attività con la costante supervisione del docente). A scuola, il telefono cellulare deve essere tenuto spento. Per motivi di emergenza, gli alunni possono sempre utilizzare il telefono della scuola. È, inoltre, fatto divieto di utilizzare qualsiasi strumento fotografico o da ripresa o da riproduzione musicale, se non espressamente autorizzati dai docenti (Regolamento d'Istituto, art. 21).

Si ricorda inoltre che il divieto di utilizzare i telefoni cellulari durante lo svolgimento delle attività di insegnamento riguarda anche il personale docente, in considerazione dei doveri derivanti dal CCNL vigente e dalla necessità di assicurare, all'interno della comunità scolastica, le migliori condizioni per lo svolgimento sereno ed efficace delle attività didattiche, unitamente all'esigenza educativa di offrire agli studenti un modello di riferimento esemplare da parte degli adulti.

Le infrazioni possono essere rilevate da tutto il personale scolastico nell'esercizio delle proprie funzioni, nonché da studenti e studentesse e dai loro genitori, che ne informeranno i docenti responsabili della sicurezza online.

Per la gestione si fa riferimento al Regolamento d'Istituto (art. 21), che prevede, in base alla gravità, le seguenti azioni: se lo studente arriva in classe e si accorge di non aver spento il cellulare, chiede il permesso al docente della I ora, se lo dimentica acceso la prima volta ammonizione sul registro elettronico, la seconda volta ammonizione sul registro elettronico e relativa comunicazione verbale e/o scritta alla famiglia, la terza volta sospensione di un giorno; se a scuola lo studente accede o scrive su un social oppure fa fotografie a compagni e adulti o selfie sospensione con obbligo di frequenza, la prima volta sospensione di un giorno, la seconda volta sospensione di tre giorni, la terza volta sospensione di 5 giorni.

Gli interventi correttivi previsti saranno rapportati all'età e al livello di sviluppo degli studenti e delle studentesse e la loro finalità sarà sempre educativa (e mai punitiva), e cioè volta al ripristino di comportamenti corretti e allo sviluppo di una crescente consapevolezza delle regole sociali e delle competenze relazionali e affettive nel mondo digitale e non. Alle studentesse e agli studenti sarà offerta la possibilità di commutare le sanzioni in attività a favore della comunità scolastica (e, in

particolare, attività di ricerca e approfondimento su regolamenti e/o norme violati e socializzazione della propria esperienza con i compagni/e a fini preventivi).

Qualora le infrazioni si configurino come reati veri e propri commessi all'interno della scuola in ambito digitale, lo si segnalerà tempestivamente al Dirigente stesso, che procederà agli adempimenti di legge previsti.

Le azioni da attuare, in ogni caso in cui si sospettino attività illegali, sono: la conservazione delle prove e il fare rapporto alle autorità competenti.

Tutto il personale scolastico, pena sanzioni disciplinari e, in casi più gravi, civili e penali, è tenuto a rispettare e promuovere il rispetto delle seguenti regole: non effettuare azioni illegali e/o che possano nuocere ai minori; evitare comportamenti digitali compromettenti; non utilizzare i sistemi di condivisione (messaggi, email) per inviare materiali inappropriati (come, ad esempio, molestie e messaggi d'odio e violenti); seguire il Regolamento d'uso del laboratorio informatico; non utilizzare Internet all'interno della scuola per attività personali non legate allo svolgimento della professione; usare supporti esterni di memorizzazione dei dati considerandone l'adeguatezza e implementando corrette procedure di salvaguardia di qualsiasi file memorizzato; mettere in atto tutte le misure di sicurezza necessarie nell'utilizzo delle attrezzature e nella gestione protetta dei dati, in particolare di quelli personali; utilizzare lecitamente copyright e licenze software; rispettare tutte le condizioni d'uso di hardware e software.

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.

Il documento di e-policy si integra con gli obiettivi e i contenuti del PTOF, con particolare riferimento al piano digitale della scuola ivi incluso, con il RAV, con il Regolamento d'Istituto, con il Patto Educativo di Corresponsabilità, con il Regolamento d'uso del laboratorio informatico e con il Regolamento d'uso dei cellulari a scuola.

Pertanto, saranno previste attività volte a rendere sempre coerenti tutte le politiche e la documentazione della scuola, in ragione delle modifiche eventualmente apportate alla e-policy.

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.

Al termine di ciascun anno scolastico, l'animatore digitale e il docente referente per il cyberbullismo, con la collaborazione dei docenti funzioni strumentali dell'area 4 (Gestione risorse tecnologiche e informatiche) e con la supervisione del Dirigente Scolastico, effettuano attività di verifica dell'impatto e dell'efficacia della e-policy nella scuola.

Dette attività includono anzitutto l'analisi degli eventuali casi problematici rilevati e della loro gestione, nonché delle segnalazioni e delle richieste da parte dei docenti, degli studenti e delle studentesse e dei loro genitori, anche in base alla introduzione di nuove tecnologie.

Se i riscontri dovessero rivelarsi insufficienti, si predisporranno questionari da somministrare ai docenti, allo scopo di far insorgere eventuali problematiche e richieste non altrimenti palesatesi.

Sulla base di quanto analizzato, se constatata l'opportunità di modifiche e/o integrazioni, all'inizio dell'anno scolastico successivo, si provvederà all'aggiornamento della e-policy d'istituto.

L'adeguatezza del documento verrà monitorata in via straordinaria, nel corso dell'anno scolastico, ogni volta che si verifichino cambiamenti significativi delle tecnologie in uso nella scuola e/o vengano emanate nuove indicazioni dal Miur, dall'Unione Europea e dal SIC Italy.

Tutte le modifiche, supervisionate dal Dirigente Scolastico, saranno presentate al Collegio Docenti e ratificate dal Consiglio d'Istituto, per garantire che tutta la comunità scolastica condivida la e-policy d'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.
- Organizzare incontri per la consultazione degli studenti/studentesse sui temi dell'ePolicy per cui si evidenzia la necessità di regolamentare azioni e

comportamenti.

- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i genitori dell'Istituto per la stesura finale dell'ePolicy.
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto agli studenti
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai docenti
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai genitori
- 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

Azioni da svolgere nei prossimi 3 anni:

- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i docenti dell'Istituto per la stesura finale dell'ePolicy.
- Organizzare incontri per la consultazione degli studenti/studentesse sui temi dell'ePolicy per cui si evidenzia la necessità di regolamentare azioni e comportamenti.
- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i genitori dell'Istituto per la stesura finale dell'ePolicy.
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto agli studenti
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai docenti
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai genitori
- 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 curriculum

2.1. Curriculum 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 curriculum digitale.

Le Indicazioni Nazionali del 2012, richiamando la Raccomandazione Europea del 2006 per il Lifelong Learning, pongono le competenze digitali tra le competenze chiave da certificare al termine del primo ciclo. Per questo, il curriculum verticale del nostro istituto promuove lo sviluppo delle competenze d’uso delle tecnologie dell’informazione e della comunicazione, cui concorrono non solo abilità più strettamente tecniche, ma anche critiche, di analisi, controllo e verifica di dati e informazioni (per valutarne l’attendibilità e l’appropriatezza) e di interazione (per una partecipazione corretta, consapevole e attiva alla società digitale). Ciò comporta la progressiva educazione alla sicurezza online che prevede, dunque, comportamenti appropriati e il riconoscimento, l’evitamento e la capacità di segnalazione corretta di fenomeni quali il cyberbullismo o il download e l’upload di file e foto senza le necessarie autorizzazioni.

Pur implicando il piano digitale della nostra scuola un aggiornamento del curriculum di Tecnologia (volto precipuamente allo sviluppo delle competenze digitali per gli studenti e le studentesse), le competenze digitali sono nel contempo perseguite anche trasversalmente a tutte le discipline del curriculum, in quanto tutte concorrono alla loro costruzione.

A questo scopo, i docenti hanno la possibilità di implementare attività didattiche sulla sicurezza online mediante l'utilizzo di appositi kit messi a disposizione della scuola dal progetto Generazioni Connesse (www.generazioniconnesse.it).

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.

Il corpo docente del nostro istituto possiede in genere buone competenze digitali di base: utilizza il registro elettronico, corrisponde per e-mail (avendo la nostra scuola, in ottemperanza alla Legge n. 135/2012, dematerializzato le comunicazioni istituzionali), usa in genere la LIM e il computer nella didattica; mentre alcuni di loro possiedono conoscenze avanzate (in particolare, le funzioni strumentali dell'area 4).

Ma, poiché il piano digitale della scuola si pone l'obiettivo di rendere l'offerta formativa sempre più coerente con i cambiamenti della società e rispondente alle esigenze di apprendimento e agli stili cognitivi degli studenti e delle studentesse, risulta indispensabile promuovere sempre più la formazione continua dei docenti sulle TIC, volta proprio all'innovazione della didattica. Per questo, un nutrito gruppo di docenti ha partecipato a corsi di formazione anche nell'ambito di piani nazionali o organizzati dalla rete di scuole, finalizzati all'innovazione delle metodologie e delle strategie didattiche. Tra questi, il progetto "Pekit One Project: Digital Lesson" (Polo Qualità di Napoli) e il progetto "Dalla lezione all'interazione" (Microsoft,USR Campania e Polo Qualità di Napoli).

Inoltre, l'animatore digitale ha realizzato, nel corso dell'anno scolastico 2015-16, un corso di alfabetizzazione digitale per gli insegnanti della scuola dell'infanzia e primaria e, nell'anno scolastico 2017-18, ha somministrato un questionario finalizzato a rilevare i bisogni digitali di tutti docenti della scuola e a mettere conseguentemente a loro disposizione corsi di formazione e/o aggiornamento per piccoli gruppi (per consentire l'operatività e l'applicabilità immediata di quanto appreso) sull'uso del digitale nella didattica e su piattaforme e app per l'apprendimento (a partire da marzo 2018 con l'animatore digitale stesso come formatore). Sono, infine, periodicamente divulgati, sempre a cura dell'animatore digitale, corsi di aggiornamento online (anche gratuiti) per docenti.

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'adesione della scuola al progetto Generazioni Connesse consente, inoltre, a tutti i docenti della scuola anche di attingere a corsi di formazione online (dedicati a diverse aree tematiche, come l'educazione ai e con i media, l'uso delle tecnologie a scuola e l'inclusione e la partecipazione), nonché a vademecum, materiali e risorse sulla sicurezza online precipuamente rivolti alla formazione dei docenti.

Video, guide in pdf, link a siti specializzati (come appunto a quello di "Generazioni Connesse", che, a sua volta, rinvia a siti di partner, quali "Telefono Azzurro" e "Save the children") sono reperibili sul sito della scuola, nell'apposita sezione "Osservatorio cyberbullismo".

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.

I momenti di confronto informali dei docenti e della dirigenza con le famiglie, finalizzati a dare continuità alle regole e alla linea adottata dalla scuola sulla sicurezza online, sono quasi quotidiani, anche perché le modalità d'uso dello smartphone (a scuola e fuori) sono argomento di continuo dibattito. La collaborazione con le famiglie nel perseguire l'adeguatezza e la sicurezza nell'uso delle TIC viene costantemente incoraggiata anche in occasione degli incontri scuola-famiglia, collegiali, assembleari e individuali.

Inoltre, sono stati predisposti, per le famiglie, un seminario con un esperto di Telefono Azzurro e un incontro con gli esperti dell'Associazione Nirvana, finalizzati proprio a sensibilizzare i genitori perché vigilino e stabiliscano regole d'uso, nonché dialoghino con i ragazzi e le ragazze, per far emergere eventuali problematiche.

L'invito a rivolgersi agli esperti di Telefono Azzurro, in caso di dubbi e incertezze, e a consultare il sito di Generazioni Connesse (nell'apposita sezione dedicata ai genitori), oltre che durante il seminario, è anche ripetuto sul nostro sito istituzionale.

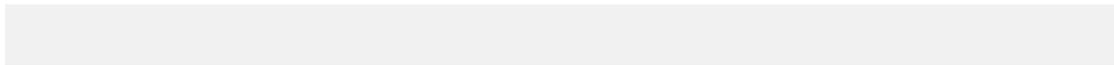
Il nostro piano d'azioni

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

- Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.

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

- Coinvolgere una rappresentanza dei genitori per individuare i temi di maggiore interesse nell'ambito dell'educazione alla cittadinanza digitale.
- 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.

In base all'art.1 D.Lgs.196/2003 della legge sulla privacy, la nostra scuola garantisce il "diritto alla riservatezza delle informazioni personali e della propria vita privata"; pertanto, i dati personali del personale scolastico e degli studenti e delle studentesse e delle loro famiglie non vengono divulgati o conferiti a terzi senza il consenso dell'interessato o di chi esercita la tutela e sono trattati nel rispetto delle regole e dei principi stabiliti dalla legge come attuativi del diritto alla privacy ([Codice in materia di protezione dei dati personali](#) - Decreto legislativo 30 giugno 2003, n.196 e successive modifiche e integrazioni).

Il Titolare del trattamento dei dati è l'Istituto I.C. Nino Cortese, nella persona del suo legale rappresentante pro tempore. Il Responsabile per la gestione e il controllo dei dati è il DSGA. Nei limiti dello svolgimento delle proprie funzioni, il personale scolastico (docente e amministrativo) è incaricato del trattamento dei dati in possesso della scuola ed è tenuto ad attenersi a criteri di correttezza, trasparenza e liceità e a non comunicarli a terzi, se non per usi di legge.

Il consenso dell'interessato o di chi ne esercita la tutela non è richiesto se si esercita per il perseguimento di specifiche finalità istituzionali ovvero quelle espressamente previste dalla normativa di settore. Viene richiesta autorizzazione al trattamento dei dati (e fornita relativa comunicazione con informativa specifica) ai genitori dei bambini/e che vengono iscritti alla scuola dell'Infanzia.

Viene, inoltre, richiesta liberatoria in cui chi ne esercita la tutela autorizza la scuola a riprendere e/o a far riprendere in video e/o a fotografare gli alunni/e, in occasione di viaggi, visite d'istruzione e partecipazione a eventi connessi all'attività didattica (da soli, con i compagni, con insegnanti e operatori scolastici), ai fini di formazione, ricerca e documentazione dell'attività didattica (come cartelloni all'interno della scuola o in occasione di esposizioni esterne); divulgazione della ricerca didattica e delle esperienze effettuate sotto forma di documento in ambiti di studio (ad es. su DVD, sul sito web della scuola o su altri siti autorizzati); stampe e giornalini scolastici; partecipazione a iniziative di sensibilizzazione alle problematiche sociali.

Tutti i membri della nostra comunità scolastica, quindi, non diffondono e comunicano i dati di altre persone (ad esempio, pubblicandoli sul web) senza averle prima informate adeguatamente e aver da loro ottenuto esplicito consenso.

I genitori potranno riprendere immagini e video di manifestazioni scolastiche, gite, recite, ma solo per utilizzo personale e se destinate all'ambito familiare. Detti immagini e video non verranno quindi mai pubblicati su Internet senza il consenso esplicito degli interessati.

Si consente agli studenti con DSA, ove previsto dal PDP, la registrazione delle lezioni, per utilizzo strettamente personale.

Gli obiettivi che il nostro istituto si impegna a soddisfare per essere conformi al Regolamento UE 2016/679 sono i seguenti

- Redigere e mantenere un registro dei trattamenti dei dati: sia per il titolare che per il responsabile dei trattamenti.

- Valutazione dei rischi sulla privacy: (definita nel regolamento Data Protection Impact Assessment o PIA) relativamente ad alcune tipologie di trattamento dei dati sensibili.
 - Analisi di processo sulla raccolta/gestione del consenso: occorre verificare che la richiesta di consenso sia chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato
 - Adozione di idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti:
 - analisi del sito web istituzionale di riferimento con proposte volte a migliorare la sicurezza e la protezione dei dati trattati:
 - progettazione del nuovo sito secondo i concetti di [privacy by default e by design](#);
 - utilizzo del protocollo HTTPS
 - utilizzo di un sistema di cifratura quando il trattamento di dati lo richiede
 - sistema di backup (sistema che permette di salvare regolarmente i dati; ripristinare eventuali file modificati o rimossi per errore dalla rete; garantire la presenza di una copia di sicurezza di tutti i file importanti);
 - proposte di messa in sicurezza della intranet scolastica:
 - sulle reti Wi-fi installate; uso di un firewall hardware (componente [hardware](#) che, utilizzando un certo insieme di regole predefinite, permette di filtrare ed eventualmente bloccare tutto il traffico da e verso una qualsiasi [rete di computer](#), lasciando passare solo tutto ciò che rispetta determinate regole);
 - istituire corsi di formazione destinati ai responsabili, agli incaricati ed eventualmente ai sub-incaricati del trattamento.
-

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.

Nello scorso anno scolastico, è stata fatta un'analisi dello status quo dei diversi plessi del nostro istituto e dei relativi bisogni. È stata implementata la rete internet in modo da coprire tutti gli ambienti non raggiunti. Rimane in sospeso il plesso dell'infanzia al Parco dei Pini dove al momento non è ancora stata portata la linea internet dall'ente locale

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.

il nostro istituto utilizza per le comunicazioni ai docenti solo una modalità formale che consiste in invio di comunicazioni all'indirizzo istituzionale nomecognome@icnincortese.edu.it. Tale veicolazione di messaggi, informazioni e aggiornamenti relativi all'attività scolastica, è regolata dalla contrattazione di Istituto.

Il registro elettronico e il sito web permettono, invece, di gestire la comunicazione con le famiglie, le quali attraverso di esso possono visualizzare molte informazioni utili, interagendo con la scuola, su:

- andamento scolastico (assenze, argomenti lezioni e compiti, note disciplinari);
- risultati scolastici (voti, documenti di valutazione);
- udienze (prenotazioni colloqui individuali);
- eventi (agenda eventi);
- comunicazione varie (comunicazioni di classe, comunicazioni personali).

il nostro istituto si impegna ad utilizzare sempre di più e meglio le potenziali di questi strumenti per rendere quanto più immediate, trasparenti ed efficaci le comunicazioni all'interno della scuola e fra scuola e famiglie.

3.4 - Strumentazione personale

I dispositivi tecnologici sono parte integrante della vita personale di ciascuno, compresa quella degli/le 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.

La nostra scuola, in collaborazione con le famiglie, si è aperta al BYOD, ossia a politiche per cui l'utilizzo di dispositivi elettronici personali durante le attività didattiche sia possibile ed efficace, pertanto già da alcuni anni, la nostra Istituzione Scolastica si è data un regolamento ampiamente condiviso attraverso tutti i canali di comunicazione.

In particolare, gli studenti e le studentesse dovranno custodire i loro cellulari e tablet spenti all'interno degli zaini e potranno utilizzarli solo dietro espressa autorizzazione dei docenti, in specifici momenti in cui è previsto dalle attività di apprendimento progettate. I cellulari possono essere di nuovo accesi solo fuori dei cancelli esterni. È fatto assoluto divieto di portare i cellulari in alcun ambiente scolastico: nei bagni, nei laboratori, in palestra e negli ambienti comuni.

Durante l'utilizzo a scopo didattico, gli studenti e le studentesse non potranno accedere a chiamate, a messaggi e a social network, o comunque usare il cellulare per comunicazioni personali.

Foto e riprese audio e/o video dovranno essere effettuate solo se previste dall'attività e se espressamente autorizzate dai docenti. Si evidenzia, in particolare, la gravità di eventuali riprese audio/video o fotografie effettuate e successivamente diffuse con l'intento di ridicolizzare

compagni/e o docenti o addirittura di intraprendere atti di cyberbullismo, che possono configurare, nei casi più gravi, gli estremi di veri e propri reati.

Gli studenti con DSA e altri bisogni educativi speciali, se previsto dal Consiglio di Classe all'interno del PDP, potranno utilizzare i loro device nelle modalità ivi approvate. Inoltre, se ratificato dal Consiglio di Classe, detto utilizzo potrà essere condiviso con gli altri alunni/e a fini inclusivi.

Durante le uscite didattiche e i viaggi di istruzione, l'uso dei cellulari è consentito al di fuori dei momenti dedicati a visite guidate e altre attività strettamente legate all'aspetto didattico dell'uscita.

La violazione di tali disposizioni configura un'infrazione disciplinare rispetto alla quale la scuola è tenuta ad applicare apposite sanzioni, come da Regolamento d'Istituto (art.21).

Anche i docenti sono tenuti a rispettare delle norme.

Non è consentito ai docenti l'utilizzo di cellulari durante le lezioni, se non a scopi didattici e a integrazione dei dispositivi in dotazione nella scuola.

La responsabilità della custodia e della corretta gestione degli strumenti personali (cellulari, tablet, ecc.) è esclusivamente a cura e di responsabilità del proprietario.

L'utilizzo del cellulare a scopi personali all'interno della scuola è consentito ai docenti e al personale ATA solo per comunicazioni urgenti, purché ciò non interferisca con il corretto svolgimento del servizio.

Il nostro piano d'azioni

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

Scegliere almeno 1 di queste azioni:

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli studenti e delle studentesse
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte dei docenti
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte del personale Tecnico Amministrativo e dagli ATA
- Organizzare uno o più eventi o attività volti a consultare i docenti dell'Istituto per redigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola
- Organizzare incontri per la consultazione degli studenti/studentesse su indicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola
- Organizzare incontri per la consultazione dei genitori su indicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola

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

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

Scegliere almeno 1 di queste azioni:

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli studenti e delle studentesse
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte dei docenti
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte del personale Tecnico Amministrativo e dagli ATA
- Organizzare uno o più eventi o attività volti a consultare i docenti dell'Istituto per redigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali.
- Organizzare incontri per la consultazione degli studenti/studentesse su indicazioni/regolamenti sull'uso dei dispositivi digitali personali
- Organizzare incontri per la consultazione dei genitori su indicazioni/regolamenti sull'uso dei dispositivi digitali personali
- Organizzare uno o più eventi o attività volti a formare il personale adulto 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 sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare i genitori dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)
- 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.

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).

L'educazione rappresenta il principale strumento di prevenzione: per questo, la scuola ha programmato numerose attività volte a sviluppare le capacità di riconoscere e gestire i rischi e i disagi online e a prevenire le problematiche derivanti da un uso poco sicuro e consapevole delle nuove tecnologie e della Rete, e, in particolare, il bullismo e il cyberbullismo, in ottemperanza all'art. 1 comma 7 della Legge 107/2015 (che individua la prevenzione e il contrasto del cyberbullismo tra gli obiettivi formativi prioritari) e delle Linee Guida della Legge 71/2017. Questa reca le "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo (e, cioè "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 online 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"). Ai sensi dell'art. 4, co. 3, l'Istituto ha individuato un docente referente con il compito di coordinare le attività di prevenzione e di contrasto del cyberbullismo.

Le attività volte a sviluppare il senso di responsabilità e il rispetto dei regolamenti nel mondo fisico e in quello digitale sono trasversali alle discipline e rafforzate da azioni finalizzate all'educazione

all'affettività, al riconoscimento e alla risoluzione dei conflitti, nonché da iniziative volte alla promozione della cultura della diversità come ricchezza e al riconoscimento che ogni persona è degna di rispetto.

Attraverso l'insegnamento-apprendimento dell'educazione civica digitale, le nostre studentesse e i nostri studenti devono essere resi consapevoli e corretti nell'uso della Rete, per non arrecare danni a se stessi e ad altri, e, per questo, viene loro insegnato a: evitare di diffondere in rete informazioni personali (come l'indirizzo di casa o la scuola che si frequenta); proteggere i propri dati sensibili, creando password complesse e non rivelandole a terzi, nonché controllando le impostazioni della privacy, se utilizzano social network; chiedere agli amici il permesso esplicito di postare immagini in cui compaiono e far sì che essi facciano altrettanto; limitare l'abitudine di postare e condividere in maniera eccessiva; usare videogiochi educativi e sicuri; informarsi in Rete con senso critico.

Per quanto concerne, in particolare, il cyberbullismo, alle studentesse e agli studenti viene poi insegnato a: non inviare messaggi violenti diretti ad accendere battaglie verbali (flaming) e/o messaggi offensivi, finalizzati a ferire (harassment); non danneggiare la reputazione degli altri (denigrazione); non spacciarsi per qualcun altro (impersonation); non rivelare informazioni private altrui (exposure e/o trickery); non escludere una persona da un gruppo online; non molestare e perseguitare online (cyberstalking).

Perché le studentesse e gli studenti acquisiscano queste competenze, è prima necessario che siano formati e/o informati i docenti e le famiglie. Quindi è caldamente richiesta la loro partecipazione alle iniziative formative e informative della scuola e la piena collaborazione nell'educazione e nella vigilanza.

Corsi di formazione e seminari su queste tematiche sono stati tenuti da un esperto di Telefono Azzurro, che, nel mese di novembre 2017, ha: aggiornato un gruppo di docenti rappresentativo dei vari plessi e segmenti della scuola; avuto un incontro informativo con i genitori, seguito da un dibattito sulle regole da condividere circa l'uso dei cellulari; tenuto corsi di formazione per gli alunni delle classi terze della scuola secondaria di primo grado.

Mediante lettera circolare (Prot.617/B10), è stato inoltre richiesto a tutti i docenti della scuola di visitare il sito del progetto Generazioni Connesse (www.generazioniconnesse.it), affinché, attraverso l'aggiornamento e l'informazione, possano attingere materiali e spunti per la didattica in classe e possano sviluppare lo scambio di consigli e suggerimenti e il confronto di esperienze tra tutti gli insegnanti della scuola, in particolare sugli aspetti relazionali delle nuove tecnologie. Anche i genitori sono stati invitati a connettersi al sito del progetto, durante gli incontri e mediante ripetuti annunci sul sito della scuola.

Nel mese di gennaio 2018, l'animatore digitale e il referente per il cyberbullismo hanno poi formato un gruppo di dieci studentesse e studenti delle classi terze e seconde della secondaria di primo grado (scelti in base alle capacità relazionali e alle competenze sul tema e tra quelli che avevano partecipato al corso Eipass), perché tenessero una lezione intitolata "Chi è il cyberbullo?" alle studentesse e agli studenti delle classi prime e seconde. Il focus della lezione era sul cyberbullismo e sui rischi derivanti da un uso non responsabile del web (evidenziando gli strumenti per la prevenzione, ma anche gli aspetti positivi della Rete come strumento di conoscenza e relazione!). Al

termine dell'esperienza di peer education, ciascuna classe ha realizzato un proprio logo word art contro il bullismo e il cyberbullismo.

Attività didattiche in classe sono state programmate per il mese di marzo 2018 anche nelle classi quarta e quinta della scuola primaria, mediante l'utilizzo degli appositi kit didattici proposti dal progetto "Generazioni Connesse".

Sono stati poi organizzati, nei mesi di febbraio e marzo 2018, per tutti i docenti, per tutti gli studenti e le studentesse della secondaria di primo grado e della scuola primaria, nonché per i loro genitori, momenti formativi con gli esperti dell'Associazione Nirvana, con la collaborazione di rappresentanti delle Forze dell'Ordine. Essi si occupano di sicurezza online (e, in particolare, di cyberstalking) e parità di genere.

Sono, inoltre, previsti, come consuetudine ad ogni anno scolastico, incontri formativi di educazione alla legalità rivolti agli studenti e alle studentesse della nostra scuola, organizzati dai Carabinieri della Caserma Stazione di Arpino, volti alla prevenzione del disagio giovanile, prestando particolare attenzione alle problematiche legate a un utilizzo non sicuro di Internet.

Nel mese di marzo si è svolta anche una visita guidata presso la Prefettura di Napoli, nell'ambito del Progetto "Istituzioni e media..incontro ai ragazzi", alla quale ha partecipato un gruppo di circa 25 studenti e studentesse delle classi terze della scuola secondaria di primo grado.

Nella programmazione del Progetto Cineforum per il prossimo anno scolastico, la referente dell'area uscite didattiche ha poi inserito tra le tematiche da trattare anche il bullismo e il cyberbullismo. Prima e dopo la visione di un film sul tema, i docenti di Lettere organizzeranno attività di approfondimento specifiche in classe.

La scuola aderisce infine alle campagne contro il bullismo e il cyberbullismo e le diffonde sul proprio sito web.

La nota MIUR del 22 gennaio 2020 con oggetto Safer Internet Day, "Together for a Better Internet - 11 febbraio 2020" ha invitato tutte le scuole a promuovere un uso più sicuro e responsabile del web e delle nuove tecnologie, in particolare tra i bambini e i giovani di tutto il mondo. "Together for a better internet"(Insieme per un internet migliore) è stato lo slogan scelto per l'edizione del 2020, ed era finalizzato a far riflettere i ragazzi non solo sull'uso consapevole della Rete, ma sul ruolo attivo e responsabile di ciascuno nella realizzazione di internet come luogo positivo e sicuro. A tal riguardo si ricorda che la nostra scuola ha in atto un progetto in collaborazione con Telefono Azzurro "Dico no al Bullismo" che ha previsto, tra l'altro, la formazione di circa 40 alunni delle nostre classi prime e seconde della scuola secondaria di I grado al fine di diventare peer educator. Quest'anno, l'11 febbraio 2020, i peer educator hanno incontrato le classi quinte della scuola primaria, hanno svolto con loro le attività della formazione (la piattaforma Generazioni Connesse, ha offerto in tal senso materiali di supporto) si sono scambiati punti di vista ed elaborato insieme nuove strategie risolutive di situazioni problematiche.

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.

Come intervenire?

Lo sviluppo delle competenze digitali e l'educazione ad un uso etico e consapevole delle tecnologie assumono quindi un ruolo centrale anche per la promozione della consapevolezza di queste dinamiche in rete. Il nostro istituto si impegna a fornire ai più giovani gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di hate speech, e promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network. Si propone di utilizzare il corso di cortometraggio di Scuola Viva che coinvolgerà gli alunni delle classi seconde e terze della scuola media nella scrittura e interpretazione di un soggetto che concorra a decostruire gli stereotipi su cui spesso si fondano forme di hate speech, in particolare legati alla razza, al genere, all'orientamento sessuale, alla disabilità; sono state programmate per ogni classe attività di educazione alla cittadinanza digitale con la finalità di promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network per favorire una presa di parola consapevole e costruttiva da parte dei giovani.

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?

Questo argomento si può affrontare in maniera trasversale, sia quando si parla di cittadinanza digitale, di cyberbullismo, di uso integrativo e non sostitutivo dei dispositivi e della Rete.

L'esperienza della Didattica a distanza ha aiutato, attraverso l'esperienza diretta, a vedere come l'integrazione della tecnologia nella didattica è un suo utilizzo funzionale che aiuta a rendere più consapevoli i ragazzi e le ragazze delle proprie abitudini online.

Si potrebbe riflettere insieme su: 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?

Per aiutare gli alunni ad un uso consapevole dei videogiochi, lo scorso anno una classe della secondaria di primo grado, in via sperimentale, ha partecipato al concorso M9 edu craft; è stata impegnata nella creazione di un mondo sostenibile per riflettere insieme su quando il videogioco si trasforma in una risorsa, sulla necessità di selezionare sempre contenuti adeguati all'età lasciandosi guidare dagli adulti di riferimento e sul tempo di utilizzo.

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

È importante, quindi, non demonizzare la tecnologia o il gioco, ma cercare di entrare nel mondo degli/le studenti e delle studentesse, stabilendo chiare e semplici regole di utilizzo.

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 medialmente 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.

Un tema così delicato può essere affrontato solo con i/le ragazzi/e della secondaria di primo grado (classi II e III). Saranno utilizzati gli strumenti offerti dal sito Generazioni Connesse.

4.6 - Adescamento online

Il **grooming** (dall'inglese "groom" - curare, prendersi cura) rappresenta una tecnica di manipolazione psicologica che gli adulti potenzialmente 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.

Sarà pertanto portato 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).

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](#).

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

Utilissima sarà un'attività educativa sull'affettività e le relazioni, aiutando a comprendere sempre la necessità di rivolgersi ad un adulto quando qualcosa online mette a disagio.

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.

Si valuterà l'opportunità di fare un'attività di sensibilizzazione rivolta ai genitori e al personale scolastico, promuovendo i servizi delle hotline anche attraverso la sezione [Vademecum](#) di Generazioni Connesse.

Il nostro piano d'azioni

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

- Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse.
- Promuovere incontri e laboratori per studenti e studentesse dedicati all' Educazione Civica Digitale.
- Pianificare e realizzare progetti di peer-education - sui temi della sicurezza online - nella scuola.

Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

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

Questa sezione dell'ePolicy contiene le procedure standardizzate per la segnalazione e gestione dei problemi connessi a comportamenti online a rischio di 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/le studenti/esse coinvolti/e (e quindi valutare se rivolgersi ad un servizio deputato ad offrire un supporto psicologico e/o di mediazione).
- **Adescamento online:** se si sospetta un caso di adescamento online è opportuno, innanzitutto, fare attenzione a non cancellare eventuali prove da smartphone, tablet e computer utilizzati dalla persona minorenne e inoltre è importante non sostituirsi al bambino/a e/o adolescente, evitando, quindi, di rispondere all'adescatore al suo posto). È fondamentale valutare il benessere psicofisico dei minori e il rischio che corrono. Vi ricordiamo che l'attuale normativa prevede che la persona coinvolta in qualità di vittima o testimone in alcune tipologie di reati, tra cui il grooming, debba essere ascoltata in sede di raccolta di informazioni con l'ausilio di una persona esperta in psicologia o psichiatria infantile.
- **Sexting:** nel caso in cui immagini e/o video, anche prodotte autonomamente da persone minorenni, sfuggano al loro controllo e vengano diffuse senza il loro consenso è opportuno adottare sistemi di segnalazione con l'obiettivo primario di tutelare il minore e ottenere 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 analogha richiesta al Garante per la protezione dei dati personali, che rimuoverà i contenuti entro 48 ore.

Vi suggeriamo, inoltre, i seguenti servizi:

- Servizio di [Helpline 19696](#) e [Chat di Telefono Azzurro](#) per supporto ed emergenze;
- [Clicca e segnala di Telefono Azzurro](#) e [STOP-IT di Save the Children Italia](#) per segnalare la presenza di materiale pedopornografico online.

Il referente per le situazioni sopra segnalate è la prof.ssa Elena Marchitelli; con lei si ricordano i docenti referenti dei diversi plessi della scuola primaria e secondaria di I grado

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](tel:19696).

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.

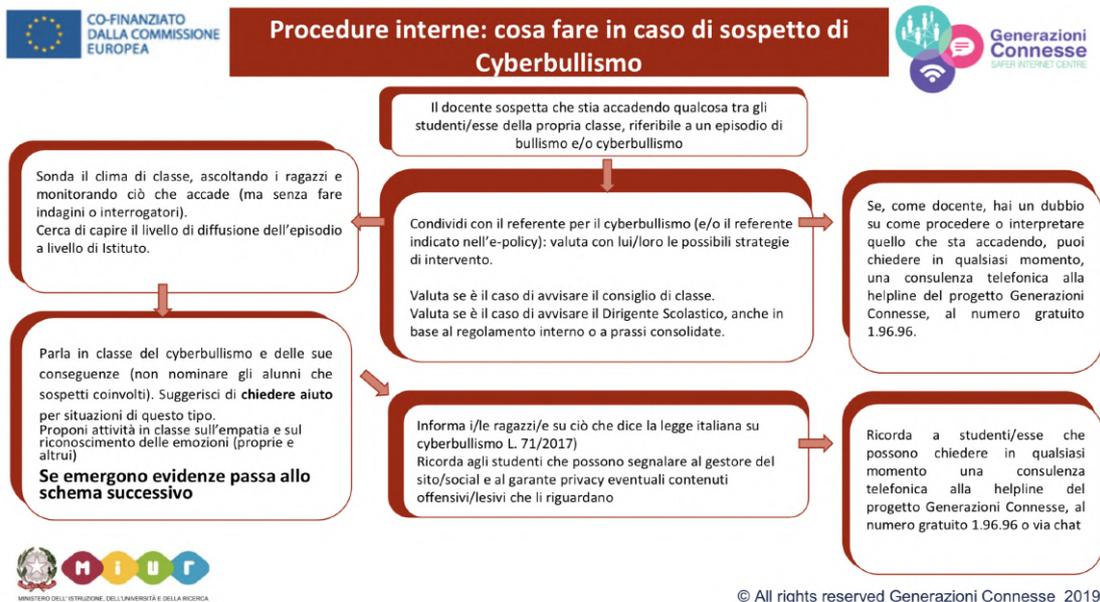
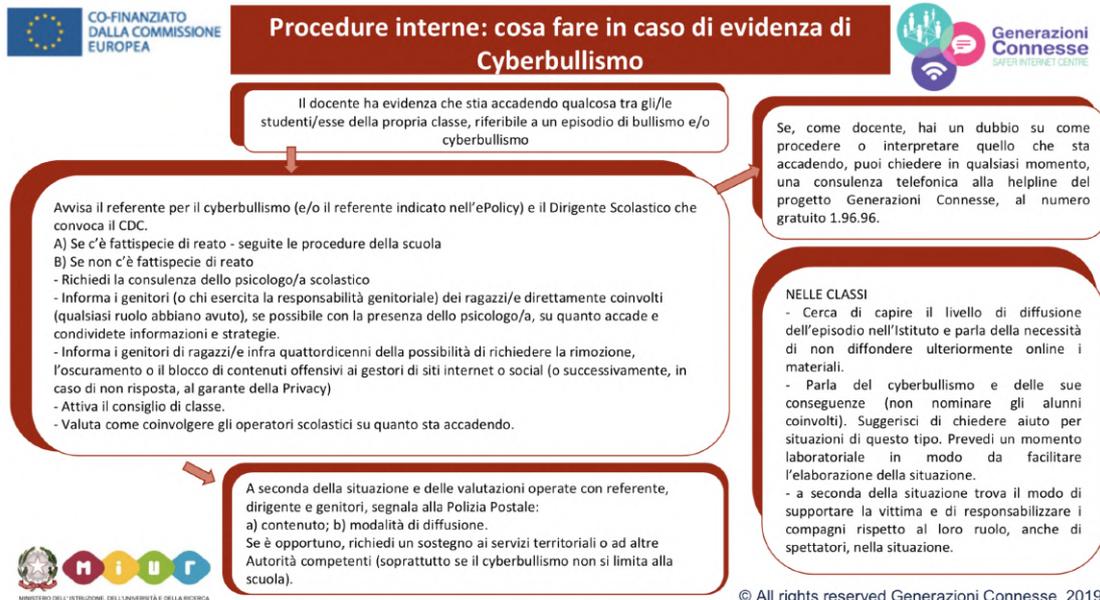
Per una mappatura degli indirizzi di tali strutture è possibile consultare il [Vademecum](#) di Generazioni Connesse “Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all’utilizzo delle tecnologie digitali da parte dei più giovani” (seconda parte, pag. 31), senza 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.

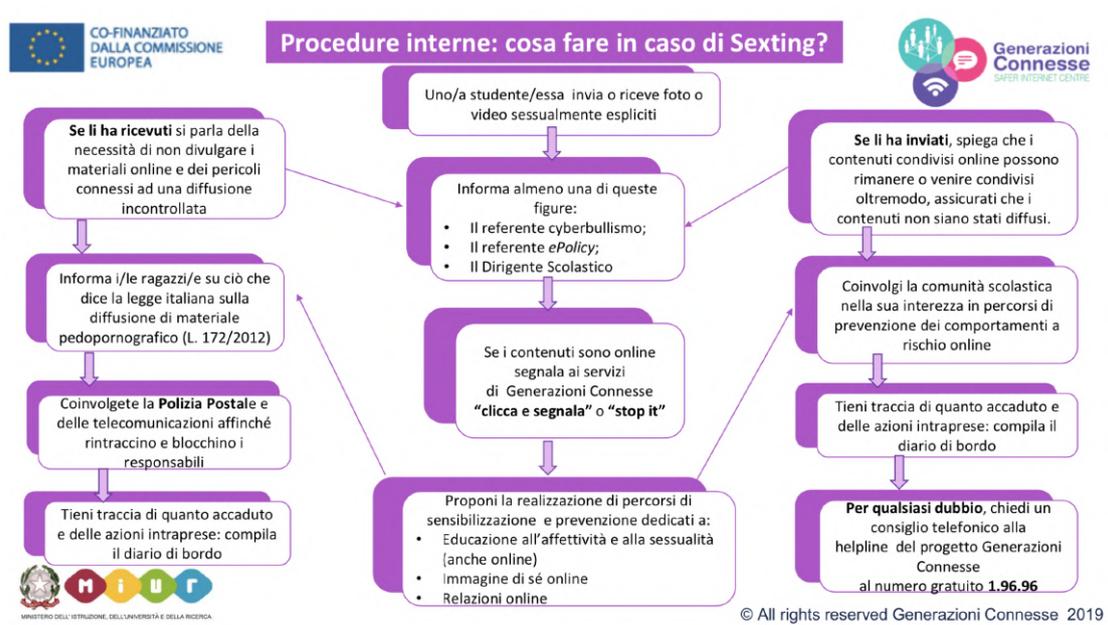
- **Comitato Regionale Unicef:** laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell’infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni):** svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare 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

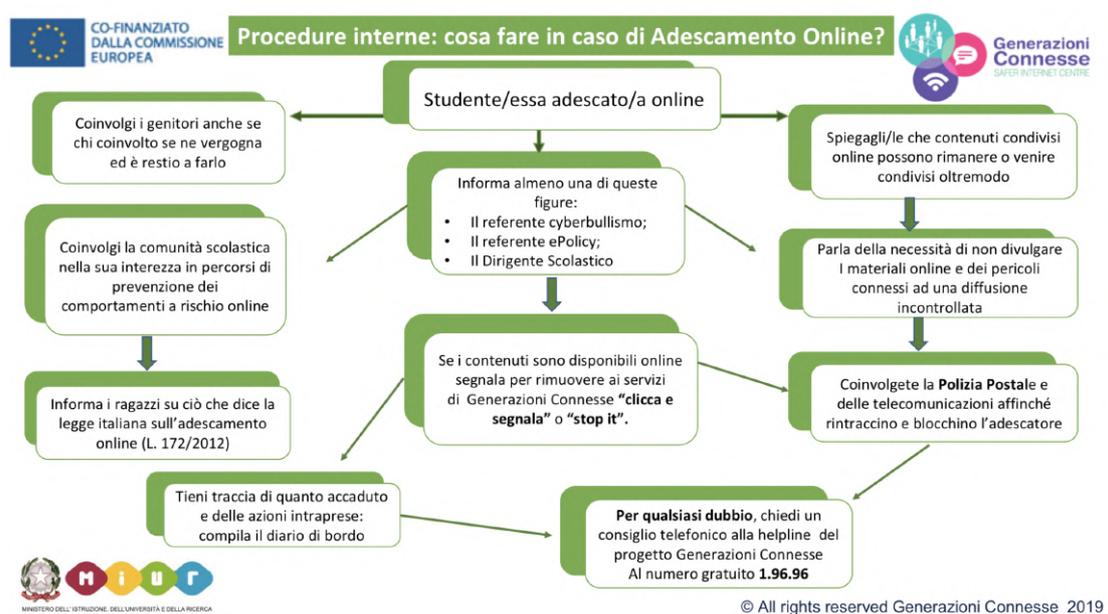
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



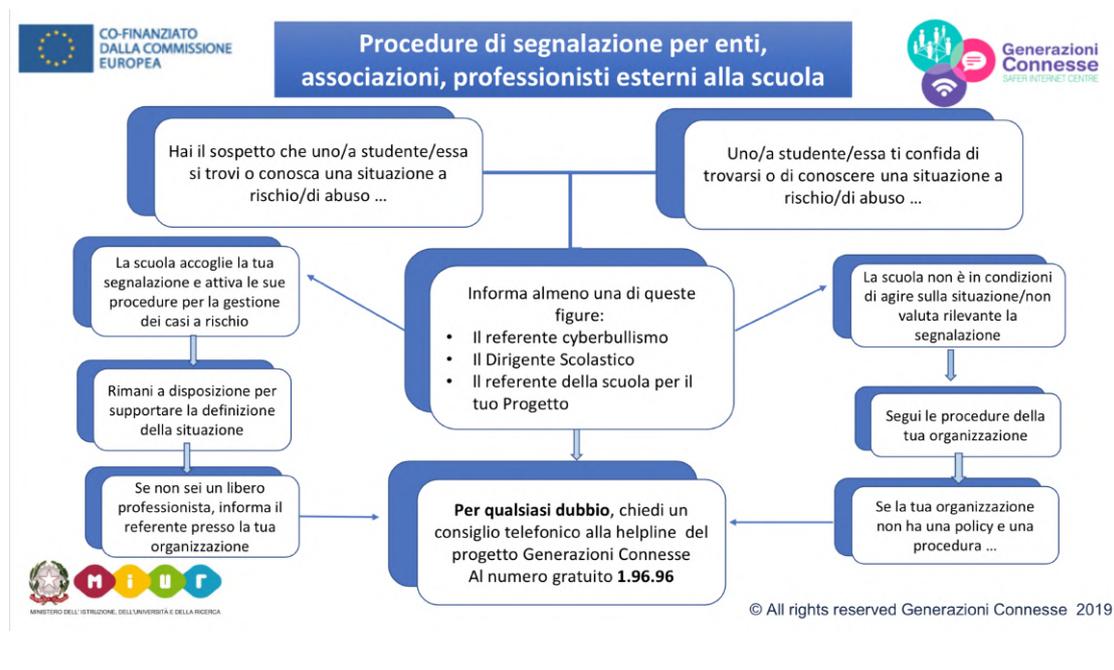
Procedure interne: cosa fare in caso di sexting?



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

Come negli anni precedenti la nostra istituzione scolastica continuerà la collaborazione con i volontari del Telefono Azzurro che hanno condotto laboratori con i ragazzi della scuola secondaria di I grado al fine di realizzare attività di peer education con i più piccoli del nostro Istituto. L'informazione è l'azione principale da realizzare per aiutare i nostri alunni a conoscere i pericoli del web e le sue insidie. Questo, unitamente a una formazione costante dei docenti sul tema, contribuirà a creare una cultura della sicurezza nell'uso delle nuove tecnologie, strumento fondamentale per la crescita della nostra società.

