



Istituto Comprensivo Statale "Nino Di Maria"
Sommatino-Delia (CL)

Via Garibaldi 9, 93019 Sommatino
Via Droce 8, 93010 Delia
Tel: 0922 871147 (Sommatino)
Tel: 0922 820290 (Delia)

e-mail: CLIC815002@istruzione.it - PEC: CLIC815002@pec.istruzione.it



Documento di ePolicy

CLIC815002

"N. DI MARIA" SOMMATINO - DELIA

VIALE GARIBALDI 9 - 93019 - SOMMATINO - CALTANISSETTA (CL)

Dirigente Scolastico Giovanna AMBROSIANO

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. Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica
4. Gestione delle infrazioni alla ePolicy
5. Monitoraggio dell'implementazione dell'ePolicy e suo aggiornamento
6. Integrazione dell'ePolicy con regolamenti esistenti

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

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.

In attuazione della Legge 71/2017 art. 1, l'I.C. Nino Di Maria di Sommatino- Delia, anche in relazione alla partecipazione al progetto di redazione della E-policy attraverso "Generazioni Connesse", predispose la presente policy per garantire l'attuazione degli interventi per contrastare il fenomeno del cyberbullismo in tutte le sue manifestazioni. Lo scopo del documento di E-policy è quello di descrivere un insieme di regolamenti, linee di azione e attività per gestire vantaggi e svantaggi della rete internet, guardando sia alle sue potenzialità in ambito didattico (cioè favorendo le misure atte a facilitare e promuovere l'utilizzo positivo delle TIC nella didattica e negli ambienti scolastici), che alla prevenzione dei rischi (cioè adottando misure di prevenzione e misure di gestione di situazioni problematiche relative all'uso delle tecnologie digitali). In particolare, il documento ha come fine la realizzazione di uno strumento operativo per evitare l'esposizione degli alunni a contenuti inappropriati o non autentici, a violazione della privacy, al bullismo on-line, a forme di ludopatia, all'utilizzo improprio, perché inconsapevole, di posta elettronica, messaggistica istantanea, blog, sms, WhatsApp e altre modalità social in cui possono veicolare contenuti "dannosi" e "diffamatori". Occorre formare e sensibilizzare docenti, genitori e alunni su atteggiamenti, relazioni, approcci che apparentemente vengono giustificati e argomentati come "leggerezze" o "scherzi", ma che possono essere invece talvolta azioni capaci di denigrare, diffamare e ferire l'individualità e la personalità dell'altro in un ambiente i cui confini sono globali. Bullismo e cyberbullismo sono i pericoli attuali legati alla condizione sociale e tecnologica del nostro tempo.

La Scuola ha come finalità non solo la formazione didattica e culturale degli studenti, ma anche intenti educativi e formativi che si esplicano attraverso la trasmissione di valori quali il rispetto dell'altro e la costruzione di relazioni "sane", prive di vessazioni, discriminazioni, atti di violenza.

Promuovere l'acquisizione di abilità pro-sociali e relazionali basate sul rispetto, sull'empatia e non sull'abuso di potere e sul desiderio di intimidire e di dominare; è compito di tutti coloro che si occupano a vario titolo dell'educazione dei bambini e degli adolescenti.

I docenti, consapevoli della propria responsabilità nel guidare gli alunni nelle attività online a scuola e nel proporre una condotta adeguata a un uso critico e consapevole di internet anche a casa, sensibilizzeranno gli studenti con percorsi didattici, su misura per ciascuna classe, mediante letture, film, video e dibattiti, tra docenti stessi e alunni e talora con esperti.

I docenti si impegnano altresì a:

- assumersi la responsabilità di segnalare prontamente eventuali malfunzionamenti o danneggiamenti alle figure preposte;
- non divulgare le credenziali di accesso agli account (username e password)

e/o, nel caso ne siano a conoscenza, alla rete Wi-Fi;
- non allontanarsi dalla postazione lasciandola incustodita, se non prima di aver effettuato la disconnessione;
- non salvare sulla memoria locale della postazione di classe file contenenti dati personali e/o sensibili.

Le strategie previste dalla scuola per garantire la sicurezza in rete sono le seguenti:

- formazione per un uso consapevole delle TIC rivolta agli insegnanti, per esempio mediante i corsi offerti dal progetto Generazioni Connesse;
- coinvolgimento dei genitori come partner educativi nei percorsi di formazione che riguardano gli studenti;
- controllo (una tantum e/o all'evenienza di episodi dubbi) del sistema informatico (cronologia, cookies, ecc.) da parte dei responsabili;
- installazione di firewall sull'accesso Internet;
- presenza di un docente o di un adulto responsabile durante l'utilizzo di Internet, della piattaforma o di altre TIC;
- aggiornamento periodico del software antivirus e scansione delle macchine in caso di sospetta presenza di virus;
- utilizzo di penne USB, CD/DVD o altri dispositivi esterni personali, solo se autorizzati dai docenti

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.

Vengono individuati i seguenti ruoli e le principali responsabilità correlate, in linea con le direttive ministeriali del 29 maggio 2017 (legge 71/2017);

1.2.1 Dirigente Scolastico

deve garantire la sicurezza (tra cui la sicurezza online) di tutti membri della comunità scolastica. Nomina il referente nonché i membri del gruppo di lavoro per il contrasto al bullismo e al cyberbullismo, per garantire la tutela degli aspetti legali riguardanti la privacy e la tutela dell'immagine di tutti i membri della comunità scolastica; per garantire

ai propri docenti una formazione di base sulle Tecnologie dell'Informazione e della Comunicazione (ICT) che consenta loro di possedere le competenze necessarie all'utilizzo di tali risorse; per garantire l'esistenza di un sistema che consenta il monitoraggio e il controllo interno della sicurezza on line.

È il dirigente Scolastico che regola il comportamento degli studenti ed impone sanzioni disciplinari in caso di comportamento inadeguato e in caso di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali.

1.2.2 L'Animatore Digitale

ed il suo team assumono la responsabilità di pubblicare sul sito della scuola e diffondere la sua conoscenza a tutti i livelli attraverso azioni significative la E-Safety Policy. 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" (con riferimento, ad esempio, allo sviluppo delle competenze digitali previste anche nell'ambito dell'educazione civica).

Monitora e rileva eventuali episodi o problematiche connesse all'uso delle TIC a scuola, e 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).

1.2.3 Il Referente bullismo e cyberbullismo

Presso l'I.C. Nino Di Maria, il Dirigente ha individuato fra i docenti un referente con il compito di coordinare le iniziative di prevenzione e di contrasto del cyberbullismo, anche avvalendosi della collaborazione delle Forze di polizia nonché delle associazioni e dei centri di aggregazione giovanile presenti sul territorio.

Il docente referente, formato attraverso le piattaforme Generazioni Connesse ed Elisa si sta occupando della redazione della presente e-policy attraverso l'adesione all'iniziativa "Generazioni connesse".

In particolare, il Referente per il bullismo e cyberbullismo d'Istituto:

- Supporta il dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d'istituto), atti e documenti.
- Coordina iniziative di prevenzione e contrasto del cyberbullismo messe in atto dalla scuola;
- Predisporre un documento di rilevazione di incidenti di sicurezza in rete;
- Facilita la formazione e la consulenza di tutto il personale.

1.2.4 I Docenti

- provvedono personalmente alla propria formazione/aggiornamento sull'utilizzo del digitale con particolare riferimento alla dimensione etica (tutela della privacy, rispetto dei diritti intellettuali dei materiali reperiti in Internet e dell'immagine degli altri: lotta al cyberbullismo);
- Supportano gli alunni nell'utilizzo consapevole delle tecnologie informatiche utilizzate a scopi didattici;

- Segnalano al Dirigente scolastico e ai suoi collaboratori eventuali episodi di violazione delle norme di comportamento stabilite dalla scuola, avviando le procedure previste in caso di violazioni;
- Supportano ed indirizzano alunni coinvolti in problematiche legate alla rete.

1.2.5 Il personale Amministrativo, Tecnico e Ausiliario (ATA)

Il personale Amministrativo, Tecnico e Ausiliario (ATA) ha il compito di svolgere funzioni miste, ossia di tipo amministrativo, contabile, gestionale e di sorveglianza connesse all'attività delle istituzioni scolastiche, in collaborazione con il dirigente scolastico e con il personale docente tutto.

Le diverse figure impegnate, in sinergia, si occuperanno ciascuno per la propria funzione, del funzionamento dell'Istituto scolastico anche attraverso lo sviluppo della cultura digitale e dell'organizzazione del tempo scuola. Il personale ATA deve essere, 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.

1.2.6 Gli Studenti e le Studentesse

- Leggono comprendono ed accettano il documento di E-Safety Policy;
- comprendono e rispettano le norme sul diritto d'autore;
- devono avere consapevolezza delle situazioni di rischio legate alla rete, telefoni cellulari, fotocamere digitali;
- devono conoscere la politica della scuola sull'uso delle immagini;
- comprendono l'importanza di adottare buone pratiche di sicurezza on-line quando si usano le tecnologie;
- si assumono la responsabilità di un utilizzo sbagliato delle tecnologie.

1.2.7 Genitori

- contribuiscono, in sinergia con il personale scolastico, alla sensibilizzazione dei propri figli sul tema della sicurezza in rete;
- incoraggiano l'impiego delle ICT da parte degli alunni nello svolgimento dei compiti a casa, controllando che tale impiego avvenga nel rispetto delle norme di sicurezza;
- agiscono in modo concorde con la scuola per la prevenzione dei rischi e l'attuazione delle procedure previste in caso di violazione delle regole stabilite;
- rispondono per gli episodi commessi dai figli minori a titolo di culpa in educando (articolo 2048 del Codice civile). Sono esonerati da responsabilità solo se dimostrano di non aver potuto impedire il fatto. Ma nei casi più gravi per i giudici l'inadeguatezza dell'educazione impartita ai figli emerge dagli stessi episodi di bullismo, che per le loro modalità esecutive dimostrano maturità ed educazione carenti.

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

Gli Enti educativi esterni e le associazioni che entrano in relazione con la scuola devono conformarsi alla politica della stessa riguardo all'uso consapevole della Rete e delle TIC; devono, inoltre,

- promuovere comportamenti sicuri,
- la sicurezza online e assicurare la protezione degli studenti e delle studentesse durante le attività che si svolgono insieme.

A talune suggeriamo di prevedere una sezione specifica dell'ePolicy con indicazioni ad hoc e procedure standard per gli attori esterni.

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.

La E-Safety Policy è un documento condiviso da tutte le componenti educative che operano nella scuola:

- è condivisa, approvata e pubblicata dal Dirigente Scolastico;
- è stesa dal referente individuato, in collaborazione con il gruppo di lavoro sul cyberbullismo e con l'Animatore Digitale;
- è letta, approvata, condivisa e deliberata dal Collegio docenti; • è approvata e deliberata dal Consiglio di Istituto;
- è pubblicata nella sezione della documentazione sul sito della scuola, al fine di essere condivisa con i genitori e con gli alunni;
- è applicata dai Consigli di classe;

- è rinnovata periodicamente attraverso le osservazioni ad essa rilevate e per adattarsi alle innovazioni che si presenteranno.

Sarà altresì condivisa con le famiglie mediante il Patto di Corresponsabilità all'inizio di ogni anno scolastico, sottoscritto dalle stesse, che si impegnano a tenervi fede.

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

Un ruolo importante potrà essere svolto dal regolare monitoraggio dello Sportello d'Ascolto, gestito dallo psicologo della scuola.

In caso venga individuata una violazione, il docente che ne venga a conoscenza, fermi in ogni caso gli obblighi di legge a suo carico, è tenuto a rivolgersi in primo luogo al Referente d'Istituto per il contrasto al bullismo e al cyberbullismo, che a sua volta ha il compito di coordinare le iniziative da mettere in atto (art. 3 comma 3 legge 71/2017) e informare il Dirigente Scolastico.

Il Dirigente, sentiti i soggetti sopra citati e acquisiti gli elementi necessari alla valutazione delle circostanze di fatto, convoca i genitori/tutori legali degli studenti coinvolti; in ogni caso il Dirigente si riserva, ove ritenuto necessario, le segnalazioni alle autorità competenti, come previsto dall'art. 5 della Legge 71/2017.

I provvedimenti disciplinari da adottare da parte del consiglio di classe nei confronti dell'alunno che ha commesso un'infrazione alla policy (in proporzione sia all'età dello studente sia alla gravità dell'infrazione commessa) potranno essere:

- richiamo verbale;
- sanzioni estemporanee commisurate alla gravità della violazione commessa (assegnazione di attività aggiuntive da svolgere a casa su temi di Cittadinanza e Costituzione, sequestro dello strumento informatico o comunicativo usato, etc);
- nota informativa ai genitori o tutori mediante registro elettronico;
- convocazione dei genitori o tutori per un colloquio con l'insegnante; • convocazione dei genitori o tutori per un colloquio con il Dirigente scolastico.

Nel caso si tratti di un reato è necessario che il Dirigente informi le autorità competenti (polizia postale).

1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

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

Il monitoraggio dell'implementazione della policy e del suo eventuale aggiornamento sarà curato dal Dirigente scolastico con la collaborazione dell'Animatore digitale. Sarà finalizzato a rilevare la situazione iniziale delle classi e gli esiti a fine anno, in relazione all'uso sicuro e responsabile delle tecnologie digitali e di internet. Il monitoraggio sarà rivolto anche ai docenti, al fine di valutare l'impatto della policy e la necessità di eventuali miglioramenti. L'aggiornamento della policy sarà curato dal Dirigente scolastico, dall'Animatore digitale, dagli Organi Collegiali, a seconda degli aspetti considerati.

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.

La policy è coerente con quanto stabilito dalla Legge ("Statuto delle studentesse e degli studenti della scuola secondaria" DPR 24 giugno 1998 n. 249, modificato dal DPR 21 novembre 2007 n. 235; Legge 29 maggio 2017 n. 71 "Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo"; Legge 31 dicembre 1996 n. 675 "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali") dal Regolamento vigente di Istituto e dal Patto di Corresponsabilità.

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 1 evento di presentazione del progetto Generazioni Connesse rivolto ai docenti
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai docenti

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 nuove tecnologie devono divenire strumento e modalità di costruzione del sé e di relazione con gli altri, pertanto dobbiamo pensare alle TIC come: canale, mezzo, strumento e forma di rappresentazione; le nuove tecnologie possono mediare le relazioni e al contempo si possono educare i nuovi cittadini ad avere delle relazioni consapevoli con le tecnologie.

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

- Conoscere e collegare le periferiche di input e output dei diversi dispositivi tecnologici presenti nella scuola (tastiera, mouse, scanner, schermo del PC, schermo LIM, audio, stampante, ecc.)
- Creare e spostare cartelle
- Creare e modificare documenti di scrittura, inserire immagini
- Creare e modificare altri tipi di documenti in base alle proposte didattiche delle diverse discipline (immagini, video, fogli di calcolo, presentazioni in Power Point, documenti di Geogebra, mappe create con Cmap o Mappe SuperEvo, Ipertesti ecc.)
- Archiviare correttamente i documenti creati nel PC (in apposite cartelle) e in altri dispositivi mobili (chiave USB, CD, DVD)
- Stampare un documento
- Utilizzare Internet per reperire informazioni funzionali allo studio con la consapevolezza che sia necessario verificare sempre se la fonte da cui si sta attingendo l'informazione sia attendibile
- Acquisire criteri per verificare l'attendibilità di una fonte
- Conoscere e rispettare le norme relative ai copyright, consapevoli delle sanzioni che derivano da un utilizzo non appropriato dei materiali reperiti in rete
- Conoscere i principali canali di condivisione delle informazioni (piattaforme online, chat, blog, social network)

- Essere consapevoli che l'identità digitale di coloro con cui condividiamo le informazioni on-line potrebbe non coincidere con quella reale. Diffidare quindi delle "amicizie" on-line con soggetti sconosciuti.
 - Conoscere i fenomeni del cyberbullismo, sexting, grooming
 - Conoscere il codice etico da rispettare on-line ed essere consapevoli delle conseguenze di comportamenti inadeguati
 - Saper individuare e segnalare agli adulti di riferimento comportamenti inadeguati osservati in rete, specialmente se reiterati nel tempo
 - Essere consapevoli dei rischi connessi alla pubblicazione on-line di foto, video e dati personali propri e di altri (chat, social network, YouTube, ecc.)
 - Essere consapevoli delle possibili conseguenze legali connesse allo scaricare file senza permesso (come video e file musicali) e/o con contenuti inopportuni
-

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.

La formazione dei docenti e del personale che opera nella scuola è un importante elemento di qualità nel servizio scolastico; essa rappresenta una leva strategica per lo sviluppo culturale dell'istituzione scolastica, per il necessario sostegno agli obiettivi di cambiamento e per un'efficace politica delle risorse umane.

L'istituto si preoccupa, in coerenza con quanto previsto nel PTOF 2019/2022, di incrementare la formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica attraverso le seguenti azioni:

- Individuazione e formazione di un animatore digitale che accompagna il Dirigente Scolastico e il DSGA nell'attuazione degli obiettivi e delle innovazioni previste dal PNSD
- Supporto da parte di un Team, già esistente, per l'innovazione, composto da docenti che collaborino con l'Animatore Digitale
- Corsi di formazione e aggiornamento interni e esterni all'Istituto su programmi e software specifici relativi alle singole discipline e/o volti all'acquisizione di competenze digitali trasversali.

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

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

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

- Partecipazione al progetto Generazioni connesse e agli eventi indicati
- Iscrizione del Referente del Cyberbullismo alla Piattaforma ELISA (Formazione in E-Learning degli Insegnanti sulle Strategie Antibullismo), raccolta del materiale fornito dal corso in una banca dati accessibile a tutto il corpo docente
- Momenti di riflessione condivisa nei vari gruppi di lavoro
- Corsi di formazione interni all'istituto
- Autoformazione e formazione a distanza
- Partecipazione a incontri e corsi con esperti

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

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

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

- La presentazione ai Consigli di Classe e al Consiglio d'Istituto della E-safety Policy qui prodotta e la sua diffusione a tutti i genitori
- La diffusione di tutto il materiale informativo ricevuto e reperito sul tema
- La presentazione del portale www.generazioniconnesse.it e l'invito a consultarlo da parte di genitori e ragazzi

- L'organizzazione di incontri con esperti aperti a genitori, docenti e alunni
- L'inserimento nel Patto di Corresponsabilità di un riferimento all'utilizzo consapevole delle TIC e della Rete.

Il nostro piano d'azioni

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

Scegliere almeno 1 di queste azioni

- 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 consapevole e sicuro di Internet e delle tecnologie digitali.

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

Scegliere almeno 1 di queste azioni

- Coinvolgere una rappresentanza dei genitori per individuare i temi di maggiore interesse nell'ambito dell'educazione alla cittadinanza digitale.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare incontri con esperti per i 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.

Ogni docente è responsabile del proprio username e della propria password di accesso al registro elettronico e all’account di Istituto. In caso di smarrimento o dimenticanza i docenti o il personale ATA possono rivolgersi alla segreteria e far presente il problema. A tutto il personale, docente e non docente, è stato raccomandato di non salvare le password nei browser se gli strumenti vengono utilizzati da più persone e di effettuare sempre il logout dai siti a cui si accede con login e dalle caselle di posta personali. Si invitano altresì i docenti ad una custodia responsabile di tutte le credenziali di accesso con password segrete, alfanumeriche e sicure, cambiate almeno ogni tre mesi.

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.

L'IC Nino Di Maria di Sommatino e Delia dispone dell'accesso alla rete wi-fi in gran parte delle aule delle scuole appartenenti all'Istituto Comprensivo. La rete non possiede filtri particolari, anche se l'accesso a Internet è protetto dalle credenziali di accesso dei docenti che utilizzano quotidianamente i computer all'interno delle classi.

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.

La rete wi-fi possiede un sistema di navigazione grazie al quale l'utente (docente) può accedere, mediante le credenziali fornite dall'animatore digitale; inoltre è possibile l'accesso al registro elettronico utilizzando il nome utente fornito dalla scuola e di una password personalizzata. Le operazioni di gestione, configurazione, backup e ripristino sono affidate all'animatore digitale e a tecnici esterni. Tutti i docenti dell'istituto possiedono una e-mail istituzionale, che affianca quella privata.

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.

Per gli studenti il Regolamento scolastico non consente l'utilizzo del cellulare durante le lezioni, ma lo favorisce, insieme ad altri devices, in alcuni momenti di apprendimento cooperativo, ricerca, condivisione file e accessi alle piattaforme di classe sotto la supervisione dei docenti.

Per i docenti: la scuola mette a disposizione un computer personale e favorisce accesso a Internet tramite rete wi-fi.

Durante le ore delle lezioni non è consentito al personale docente l'utilizzo con finalità extrascolastiche del cellulare o di altri dispositivi elettronici, mentre è permesso l'uso di tali dispositivi elettronici personali solo a scopo didattico ad integrazione di quelli scolastici disponibili. Qualora si utilizzino a scuola dispositivi di archiviazione esterna di proprietà personale (chiavette usb, dischi fissi portatili etc.) è opportuno controllare preventivamente che essi siano esenti da virus per evitare di danneggiare le attrezzature comuni. Durante il restante orario di servizio è consentito l'utilizzo del cellulare solo per comunicazioni personali di carattere urgente, mentre è permesso l'uso di altri dispositivi elettronici personali per attività funzionali all'insegnamento, ad integrazione di quelli scolastici disponibili.

Per il personale della scuola: tutto il personale scolastico è autorizzato ad utilizzare devices personali laddove non stia assolvendo ad un ruolo didattico, a condizione che l'utilizzo non intralci il normale svolgimento delle attività scolastiche né distraiga dal corretto svolgimento delle proprie mansioni. In tal caso la responsabilità sulla conservazione e corretta gestione degli stessi è affidata unicamente al proprietario

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
- 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:

- 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

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.

Anche gli adolescenti italiani, ormai definiti nativi digitali, fanno parte di una realtà 3.0, ossia fortemente informatizzata e imbevuta di continue e talvolta incontrollate connessioni social. La scuola, consapevole della forte attrazione che le nuove tecnologie esercitano sui ragazzi e del fatto che questi non sempre conoscano i rischi legati ad un uso sregolato ed improprio di determinati mezzi, come istituzione formativa ed educativa, ha il compito morale di fornire strumenti adeguati per il discernimento, responsabile e critico, dei vari aspetti della rete.

Tra i principali rischi è opportuno considerare:

- esposizione a contenuti violenti e non adatti alla loro età;
- videogiochi diseducativi;
- pubblicità ingannevoli;
- accesso ad informazioni scorrette;
- virus informatici in grado di infettare computer e cellulari;
- rischio di molestie o maltrattamenti da coetanei (cyberbullismo);
- scambio di materiale a sfondo sessuale (sexting);
- uso eccessivo di Internet/cellulare (dipendenza);
- adescamento online (grooming).

Fondamentale quindi risulta essere il ruolo dei docenti che, come educatori, cercheranno momenti opportuni, all'interno delle programmazioni didattiche, per soffermarsi con gli alunni su tali rischi. È importante osservare le situazioni

relazionali che si sviluppano nelle classi per individuare possibili situazioni di disagio, quindi intervenire. Questo percorso interno, in un clima di rispetto e di reciproca accettazione, che i docenti porteranno avanti, potrà avvalersi della partecipazione ad iniziative esterne proposte da Enti del territorio selezionati, coerenti con le problematiche di cui sopra.

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).

La preadolescenza (10-14 anni) è di sicuro il momento in cui si manifesta in modo più intenso l'attrazione dei ragazzi verso le nuove tecnologie; il passaggio alla scuola secondaria di I grado, l'aumento dell'autonomia negli spostamenti, la forte pressione sociale esercitata dal gruppo di coetanei, l'avvio della pubertà, che comporta importanti cambiamenti fisici, sono tutti elementi che spingono i ragazzi a diventare fruitori quotidiani di tecnologia, soprattutto attraverso social network e smartphone.

Negli ultimi anni sembra sempre più anticipato l'approccio dei bambini con le nuove tecnologie: spesso è il regalo preferito per la promozione, per eventi religiosi in età pari 9/10 anni.

Gli alunni di oggi hanno ottime competenze tecniche ma, allo stesso tempo, mancano ancora di pensiero riflessivo e critico sull'uso delle tecnologie digitali e della consapevolezza dei rischi del mondo digitale.

I genitori e le scuole possono sostenere i bambini e i giovani dando loro i giusti

consigli e discutendo con loro su quali conseguenze può avere il loro comportamento in rete e cosa significhi il cybermobbing per le vittime.

Il fenomeno del cyberbullismo viene così definito dalla Legge 29 maggio 2017, n. 71 "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" (art.1).

Questa forma di bullismo (bullismo elettronico) esercitata a distanza attraverso strumenti informatici (e -mail, sms, whatsapp, chat, blog, siti internet, immagini o video diffusi in rete...), si traduce in numerose forme di aggressione e molestie, sovente accompagnate dall'anonimato ed accresciute dal fatto che la distanza del persecutore rispetto alla vittima rende più difficile la percezione della sua sofferenza.

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.

Il fenomeno di "incitamento all'odio" o "discorso d'odio", indica discorsi (post, immagini, commenti...) 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, etc.) ai danni di una persona o di un gruppo. "L'incitamento all'odio deve essere inteso, quindi, come comprensivo di tutte le forme di espressione che dividono, incitano, promuovono o giustificano l'odio razziale, la xenofobia, l'antisemitismo o altre forme di odio generate dall'intolleranza, ivi comprese: l'intolleranza espressa dal nazionalismo, e dall'etnocentrismo aggressivi, la discriminazione e l'ostilità nei confronti delle minoranze, dei migranti e delle persone con origine straniera" (www.coe.int). Tale fenomeno, purtroppo, negli ultimi anni si è

fortemente diffuso e rafforzato soprattutto attraverso l'uso della Rete, i social network in particolar modo, dove non è difficile e infrequente trovare forme di odio e hate speech online particolarmente violente. Per questo è estremamente importante affrontarlo con ragazze e ragazzi anche a scuola.

La prevenzione necessariamente passa attraverso la conoscenza del fenomeno al fine di conoscerne le caratteristiche quali:

- Il discorso d'odio procura sofferenza. La parola ferisce, e a maggior ragione l'odio! Il discorso può violare i diritti umani. Il discorso d'odio online non è meno grave della sua espressione offline, ma è più difficile da individuare e da combattere.
- Gli atteggiamenti alimentano gli atti. Il discorso dell'odio è pericoloso anche perché può condurre a più gravi violazioni dei diritti umani, e perno alla violenza fisica. Può contribuire a inasprire le tensioni razziali e altre forme di discriminazione e di violenza.
- L'odio online non è solo espresso a parole. Internet ci permette di comunicare rapidamente e in modi svariati, ad esempio, mediante i social media e i giochi online, molto spesso, d'altronde, in maniera anonima. L'odio online può esprimersi sotto forma di video e foto, come pure, più solitamente, di contenuto testuale. Le forme visive o multimediali hanno sovente un impatto più forte sugli atteggiamenti (consci e inconsci).
- L'odio prende di mira sia gli individui che i gruppi. L'odio online può prendere di mira dei gruppi che spesso sono già vulnerabili sotto altri aspetti, come i richiedenti asilo, le minoranze religiose o le persone con disabilità. Tuttavia, anche i singoli individui sono sempre maggiormente oggetto di attacchi. Le conseguenze sono talvolta fatali, come dimostrato da numerosi fatti di cronaca riferiti dai media, riguardanti giovani vittime di cyberbullismo che sono state spinte al suicidio.
- Internet è difficilmente controllabile. La diffusione di messaggi di incitamento all'odio è maggiormente tollerata su Internet rispetto al mondo offline ed è sottoposta a minori controlli. È ugualmente più facile (e comporta meno rischi) insultare o molestare online, perché le persone spesso si esprimono sotto la copertura dell'anonimato.
- Ha radici profonde. Gli atteggiamenti e le tensioni sociali che suscitano sentimenti di odio online affondano le loro radici nella società, e non sono diversi, in genere, da quelli che alimentano il discorso dell'odio offline.
- Impunità e anonimato. Sono le due presunte caratteristiche delle interazioni sociali in rete:

l'impunità e l'anonimato. Queste abbassano le remore etiche. In realtà, però, qualsiasi azione compiuta sul web consente di rintracciare il suo autore.

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?

La dipendenza da Internet, che può manifestarsi anche attraverso le ore trascorse online

a giocare, rappresenta una questione importante per la comunità scolastica che deve attenzionare il fenomeno e fornire gli strumenti agli studenti e alle studentesse anche questi siano consapevoli dei rischi che comporta l'iperconnessione. La **S.I.I.Pa.C., la Società Italiana Intervento Patologie Compulsive**, definisce la dipendenza da Internet come progressivo e totale assorbimento del soggetto alla Rete; di seguito alcune caratteristiche specifiche:

- **Dominanza.** L'attività domina i pensieri ed il comportamento del soggetto, assumendo un valore primario tra tutti gli interessi.
- **Alterazioni del tono dell'umore.** L'inizio dell'attività provoca cambiamenti nel tono dell'umore. Il soggetto prova un aumento d'eccitazione o maggiore rilassatezza come diretta conseguenza dell'incontro con l'oggetto della dipendenza.
- **Conflitto.** Conflitti inter-personali tra il soggetto e coloro che gli sono vicini, conflitti intra-personali interni a se stesso, a causa del comportamento dipendente.
- **Ricaduta.** Tendenza a ricominciare l'attività dopo averla interrotta.

I segnali patologici di questo che viene descritto come "un vero e proprio abuso della tecnologia", anche denominato "Internet Addiction Disorder" (I.A.D. coniato dallo psichiatra Ivan Goldberg 1996), sono specifici così come accade per le altre dipendenze più "tradizionali". In particolare, si hanno: la tolleranza ossia quando vi è un crescente bisogno di aumentare il tempo su internet e l'astinenza quando, cioè, vi è l'interruzione o la riduzione dell'uso della Rete che comporta ansia, agitazione psicomotoria, fantasie, pensieri ossessivi (malessere psichico e/o fisico che si manifesta quando s'interrompe o si riduce il comportamento). Tutto questo ha ripercussioni sulla sfera delle relazioni interpersonali che diventano via via più povere e alle quali si preferisce il mondo virtuale, con alterazioni dell'umore e della percezione del tempo.

Da sottolineare, la nomofobia (nomo deriva da "no-mobile") termine usato per categorizzare quei soggetti che sperimentano emozioni negative, quali ansia, tristezza e rabbia quando non sono connessi con il proprio smartphone. Spesso il trascorrere del tempo online, in termini disfunzionali, è scandito dal gioco virtuale che può anche assumere forme di Dipendenza dal gioco online (Net gaming addiction o Internet Gaming Addiction) inserito all'interno del Manuale Diagnostico Statistico dei Disturbi Mentali (DSM 5). Da specificare che la dipendenza qui si realizza quando c'è un abuso, ossia un utilizzo continuativo e sistematico della Rete al fine di giocare impegnando la maggior parte delle giornate, con la conseguente sottrazione del tempo alle altre attività quotidiane del minore. In particolare, sei sono le componenti che

a livello bio-psico-sociale possono portare ad una vera e propria dipendenza. Di seguito i sintomi che devono essere presenti (per un arco di tempo di almeno un anno):

- il giocatore è assorbito totalmente dal gioco;
- il giocatore è preoccupato e ossessionato dal gioco;
- il gioco consente alla persona di sfuggire alla realtà con la sperimentazione di emozioni più piacevoli;
- il giocatore manifesta sempre di più l'impulso di giocare e di sperimentare emozioni positive;
- il giocatore sente di dover dedicare più tempo ai giochi; il giocatore se non può giocare manifesta ansia, depressione e irritabilità;

- può emergere un ritiro sociale (si veda il punto 3);
- il giocatore, anche se comprende la gravità della situazione e sospende di giocare comunque non riesce a interrompere del tutto;
- il giocatore mente agli altri sull'utilizzo che fa dei giochi on line;
- il giocatore ha perso o mette a rischio relazioni o opportunità a causa dei giochi su Internet o ha perso interesse verso attività nella vita reale.

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

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

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

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 medialti 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.

Il sexting (abbreviazione di sex – sesso e texting – messaggiare, inviare messaggi) indica l'invio e/o la ricezione di contenuti (video o immagini) sessualmente espliciti che ritraggono se stessi o gli altri.

"Spesso sono realizzate con il telefonino, e vengono diffuse attraverso il cellulare (tramite invio di mms o condivisione tramite bluetooth) o attraverso siti, e-mail, chat. Spesso tali immagini o video, anche se inviate ad una stretta cerchia di persone, si diffondono in modo incontrollabile e possono creare seri problemi, sia personali che legali, alla persona ritratta. L'invio di foto che ritraggono minorenni al di sotto dei 18 anni in pose sessualmente esplicite configura, infatti, il reato di distribuzione di materiale pedopornografico".

I contenuti sessualmente espliciti, quindi, possono diventare materiale di ricatto assumendo la forma di "revenge porn" letteralmente "vendetta porno" fenomeno quest'ultimo che consiste nella diffusione illecita di immagini o di video contenenti riferimenti sessuali diretti al fine di ricattare l'altra parte (la Legge 19 luglio 2019 n. 69, all'articolo 10 ha introdotto in Italia il reato di revenge porn, con la denominazione di diffusione illecita di immagini o di video sessualmente espliciti. Si veda l'articolo 612 ter del codice penale rubricato "Diffusione illecita di immagini o video sessualmente espliciti").

Tra le caratteristiche del fenomeno vi sono principalmente:

- la fiducia tradita: chi produce e invia contenuti sessualmente espliciti ripone fiducia nel destinatario, credendo, inoltre, alla motivazione della richiesta (es. prova d'amore richiesta all'interno di una relazione sentimentale);
- la pervasività con cui si diffondono i contenuti: in pochi istanti e attraverso una condivisione che diventa virale, il contenuto a connotazione sessuale esplicita può essere diffuso a un numero esponenziale e infinito di persone e ad altrettante piattaforme differenti. Il contenuto, così, diventa facilmente modificabile, scaricabile e condivisibile e la sua trasmissione è incontrollabile;
- la persistenza del fenomeno: il materiale pubblicato online può permanervi per un tempo illimitato e potrebbe non essere mai definitivamente rimosso. Un contenuto ricevuto, infatti, può essere salvato, a sua volta re-inoltrato oppure condiviso su piattaforme diverse da quelle originarie e/o in epoche successive.

La consapevolezza, o comunque la sola idea di diffusione di contenuti personali, si replica nel tempo e può finire con il danneggiare, sia in termini psicologici che sociali, sia il ragazzo/la ragazza soggetto della foto/del video che colui/coloro che hanno contribuito a diffonderla. Due fattori, quindi, che sono fra loro strettamente legati e che rappresentano veri e propri comportamenti criminali i quali hanno ripercussioni negative sulla vittima in termini di autostima, di credibilità, di reputazione sociale off e online. A ciò si associano altri comportamenti a rischio, di tipo sessuale ma anche riferibili ad abuso di sostanze o di alcool.

I rischi del sexting, legati al revenge porn, possono contemplare: violenza psicosessuale, umiliazione, bullismo, cyberbullismo, molestie, stress emotivo che si riversa anche sul corpo insieme ad ansia diffusa, sfiducia nell'altro/i e depressione.

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.

Potenziali vittime dell'adescamento online possono essere sia bambini che bambine, sia ragazzi che ragazze. Il fenomeno, infatti, non conosce distinzione di genere. Gli adolescenti sono particolarmente vulnerabili, poiché si trovano in una fase della loro vita

in cui è molto importante il processo di costruzione dell'identità sessuale. Anche per questo potrebbero essere aperti e curiosi verso nuove esperienze e, talvolta, attratti da relazioni intime e apparentemente rassicuranti. In questa fase è importante, infatti, il bisogno di avere attenzioni esclusive da un'altra persona, di ottenere rinforzi esterni di approvazione per il proprio corpo e la propria immagine. È proprio in ragione della fiducia costruita nella relazione che le vittime di adescamento online riferiscono di sentirsi umiliate, usate, tradite e tendono a sentirsi in colpa e ad autosvalutarsi per essere cadute nella trappola. L'adescamento, quindi, non avviene apparentemente con una dinamica violenta, ma il "prendersi cura" del minore rappresenta la conditio per carpirne la fiducia ed instaurare una relazione a sfondo erotico. Può capitare che l'adescatore si presenti al minore sotto falsa identità, fingendo quindi di essere un'altra persona così da attirare maggiormente l'attenzione del minore (ad esempio, potrebbe fingersi un talent scout del mondo dello spettacolo alla ricerca di volti nuovi).

Il processo di adescamento segue generalmente 5 fasi:

- Fase dell'amicizia iniziale: Questa è la fase in cui l'adescatore cerca i primi contatti con la vittima individuata, provando a socializzare con lei. Tenterà, quindi, di conoscerla meglio al fine di scoprirne bisogni, interessi e il contesto in cui vive. Condividendo argomenti di interesse del minore l'adescatore cercherà pian piano di conquistarsi la sua fiducia, ponendogli domande frequenti che attestano interesse e attenzione nei suoi confronti. Gradualmente affronterà con la vittima argomenti sempre più privati ed intimi.
- La fase di risk-assessment: in seguito ai primi contatti con il minore, l'adescatore cerca di comprendere il contesto in cui si svolge l'interazione (es. da dove si collega alla Rete? I genitori lo controllano quando chatta? Che rapporto ha con loro?). L'obiettivo dell'adescatore è quello di rendere sempre più privato ed "esclusivo" il rapporto, cercando di passare, ad esempio, da una chat pubblica ad una privata, da una chat alle conversazioni attraverso il telefono, per poterne così carpire il numero.
- Fase della costruzione del rapporto di fiducia: le confidenze e le tematiche affrontate divengono via via più private ed intime o comunque molto personali. In questa fase l'adescatore può iniziare a fare regali di vario tipo alla vittima e può anche avvenire lo scambio di foto, subito e non necessariamente a sfondo sessuale.
- Fase dell'esclusività: l'adescatore rende la relazione con il minore sempre più "segreta", isolandolo sempre più dalla famiglia e dagli amici. Chiederà alla vittima di non raccontare a nessuno ciò che sta vivendo. L'esperienza reciproca verrà presentata come un "geloso segreto" da custodire per non rovinare tutto. In questa fase l'adescatore potrà ricorrere a ricatti morali puntando sulla fiducia costruita, sulla paura o sul senso di colpa.
- Fase della relazione sessualizzata: in questa fase la richiesta di immagini o video sempre più privati e a sfondo erotico potrebbe essere più insistente, così come la proposta di incontri offline. Qualora il minore avesse già inviato immagini o video privati, potrebbe essere ricattato dall'adescatore: se non accettasse un eventuale incontro l'adescatore potrebbe diffondere quel materiale online. Questi, inoltre, tenderà a presentare sempre la situazione come "normale" al fine di vincere le eventuali resistenze del minore a coinvolgersi in tale rapporto.

Per riconoscere un eventuale caso di adescamento online è importante prestare attenzione a piccoli segnali che possono essere indicatori importanti, come ad esempio un cambiamento improvviso nel comportamento di un minore.

A seguire, alcuni segnali e domande che potrebbero esserci di aiuto:

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

Se si sospetta o si ha la certezza di un caso di adescamento online è importante, innanzitutto, che l'adulto di riferimento non si sostituisca al minore nel rispondere, ad esempio, all'adescatore. È importante che il computer o altri dispositivi elettronici del minore vittima non vengano usati per non compromettere eventuali prove. Casi di adescamento online richiedono l'intervento della Polizia Postale e delle Comunicazioni a cui bisogna rivolgersi il prima possibile, tenendo traccia degli scambi fra il minore e l'adescatore (ad esempio, salvando le conversazioni attraverso screenshot, memorizzando eventuali immagini o video...). L'adescamento, inoltre, può essere una problematica molto delicata da gestire e può avere ripercussioni psicologiche significative sul minore. Per questo potrebbe essere necessario rivolgersi ad un Servizio territoriale (es. Consultorio Familiare, Servizio di Neuropsichiatria Infantile, ecc.) in grado di fornire alla vittima anche un adeguato supporto di tipo psicologico o psichiatrico. I minori vittime di adescamento riferiscono, generalmente, di sentirsi traditi, ma anche di provare un senso di colpa per essere caduti in trappola ed essersi dati di uno sconosciuto. Inutile sottolineare che nei casi più estremi in cui l'adescamento porta ad un incontro fisico e ad un abuso sessuale un sostegno psicologico esperto per il minore è da considerarsi prioritario e urgente.

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](#).

L'abuso sessuale online rappresenta una particolare declinazione dell'abuso sessuale su bambini/e, ragazzi/e, la cui caratteristica fondante è il ruolo ricoperto dalle tecnologie digitali, le quali diventano il mezzo principale attraverso cui l'abuso viene perpetrato, documentato e diffuso in Rete con immagini e/o video. Le dinamiche attraverso cui l'abuso sessuale online si manifesta producono effetti sulle vittime che si aggiungono e moltiplicano a quelli associati all'abuso sessuale. Si pensi, a titolo di esempio, all'impatto che può avere la consapevolezza dell'esistenza (spesso anche in Rete) delle immagini e/o video dell'abuso sulla vittima, o a come gestire le stesse immagini e/o video durante la fase investigativa e giudiziaria. L'esposizione alle immagini dell'abuso, infatti, sia durante il processo giudiziario, sia durante il percorso di cura, deve essere attentamente valutata, poiché può comportare, per il/la minore coinvolto/a, un rischio di vittimizzazione secondaria. Negli ultimi anni, infine, abbiamo assistito all'emergere di un altro fenomeno che può avere risvolti connessi al fenomeno della pedopornografia: il sexting, di cui abbiamo parlato nei precedenti capitoli. La mancanza di intenzione di danneggiare o sfruttare l'altro/a (anche se a volte tale materiale può essere successivamente utilizzato con questo scopo come nel caso del cyberbullismo o del ricatto a fini di estorsione) non esclude che i comportamenti del sexting possano configurare reati connessi con la pedopornografia poiché, secondo il nostro ordinamento giudiziario, il materiale così prodotto e scambiato si declina come pedopornografico e soprattutto perché il rischio di perdere il controllo di tali immagini, uscendo dallo scambio consensuale è molto alto e spesso ragazzi e ragazze non hanno consapevolezza delle conseguenze (anche serie) delle loro azioni, come la possibilità di diffondere in Rete immagini intime/private di altri/e fuori dai canali riservati dello scambio.

In un'ottica di attività preventive, il tema della pedopornograa è estremamente delicato, occorre parlarne sempre in considerazione della maturità, della fascia d'età e selezionando il tipo di informazioni che si possono condividere. Ad esempio, non è utile diffondere tra i bambini e le bambine più piccoli/e l'uso di servizi come le hotline, sia perché in caso di visione accidentale di materiale pedopornografico è opportuno che bambini/e e ragazzi/e possano parlarne con gli adulti di riferimento per la migliore risposta possibile, sia perché si potrebbe incentivare la ricerca proattiva, che comunque è vietata

dalla legge italiana, per minori e per adulti. Risulta utilissima l'attività educativa sull'affettività e le relazioni, sottolineando 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.

Inoltre, è auspicabile che possa rientrare nei temi di un'attività di sensibilizzazione rivolta ai genitori e al personale scolastico, promuovendo i servizi delle hotline.

Il nostro piano d'azioni

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

Scegliere almeno 1 di queste azioni:

- Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse.

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

Scegliere almeno 1 di queste azioni:

- 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.

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 un/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 dai/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 minorenni e inoltre è importante non sostituirsi al bambino/a e/o adolescente, evitando, quindi, di rispondere all'adescatore al suo posto). È fondamentale valutare il benessere psicofisico dei minori e il rischio che corrono. Vi ricordiamo che l'attuale normativa prevede che la persona coinvolta in qualità di vittima o testimone in alcune tipologie di reati, tra cui il grooming, debba essere ascoltata in sede di raccolta di informazioni con l'ausilio di una persona esperta in psicologia o psichiatria infantile.
- **Sexting**: nel caso in cui immagini e/o video, anche prodotte autonomamente da persone minorenni, sfuggano al

loro controllo e vengano diffuse senza il loro consenso è opportuno adottare sistemi di segnalazione con l'obiettivo primario di tutelare il minore e ottenere la rimozione del materiale, per quanto possibile, se online e il blocco della sua diffusione via dispositivi mobili.

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

Vi suggeriamo, inoltre, i seguenti servizi:

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

Il docente di classe, poiché trascorre diverse ore con i propri alunni, di solito è colui che potrebbe accorgersi per primo di comportamenti anomali, riconducibili a un disagio. Per questo potrà segnalare e tenere nota di situazioni particolari, mediante il DIARIO DI BORDO (Allegato C). Ulteriore strumento di indagine potrebbe rivelarsi la somministrazione di un sondaggio per rilevare episodi di bullismo e cyberbullismo tra i ragazzi (Allegato B).

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).

Il docente, l'ATA o lo psicologo, che abbia effettivamente riscontrato o che sia venuto a conoscenza di un episodio o una situazione di disagio, potrà, anche mediante il MODULO DI SEGNALAZIONE (Allegato A), informare sia il Referente per il bullismo e cyberbullismo sia il Dirigente Scolastico.

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.

L'Ufficio Scolastico Regionale: supporta le scuole in attività di prevenzione ed anche nella segnalazione di comportamenti a rischio correlati all'uso di Internet.

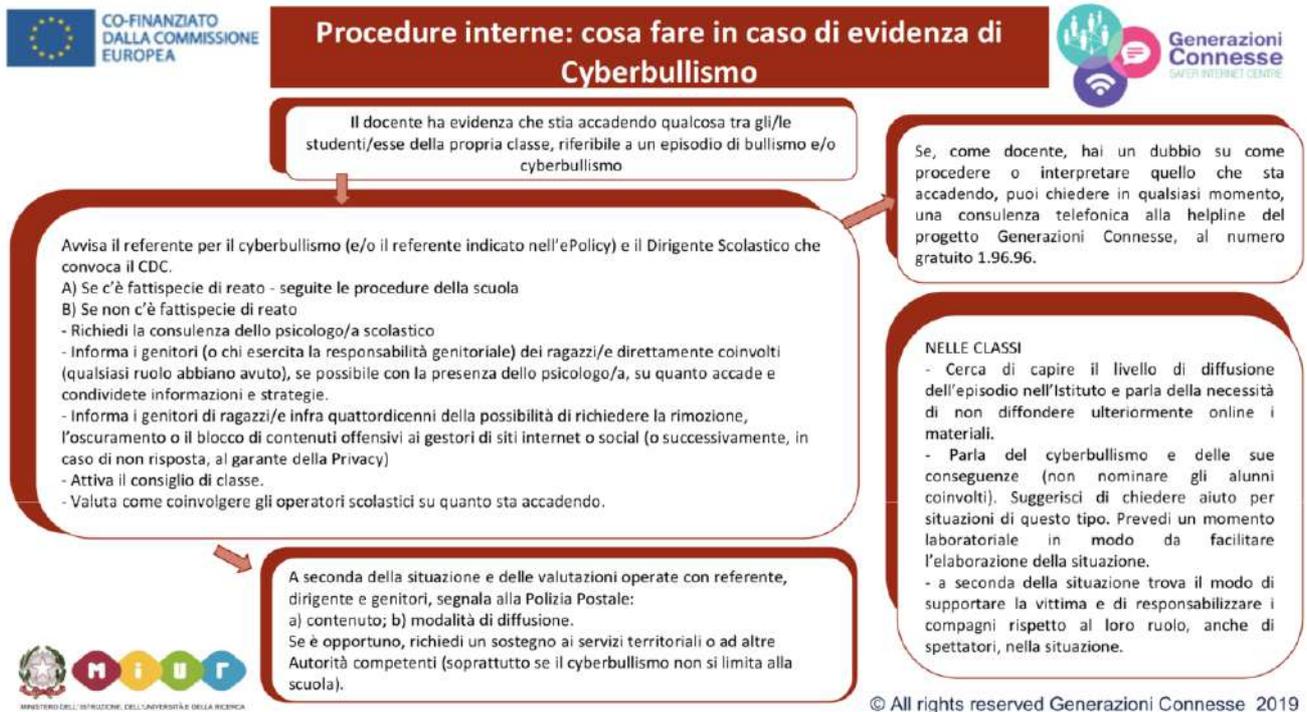
La Polizia Postale e delle Comunicazioni : accoglie tutte le segnalazioni relative a comportamenti a rischio nell'utilizzo della Rete e che includono gli estremi del reato.

Le Aziende Sanitarie Locali: forniscono supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in Rete. In alcune regioni,

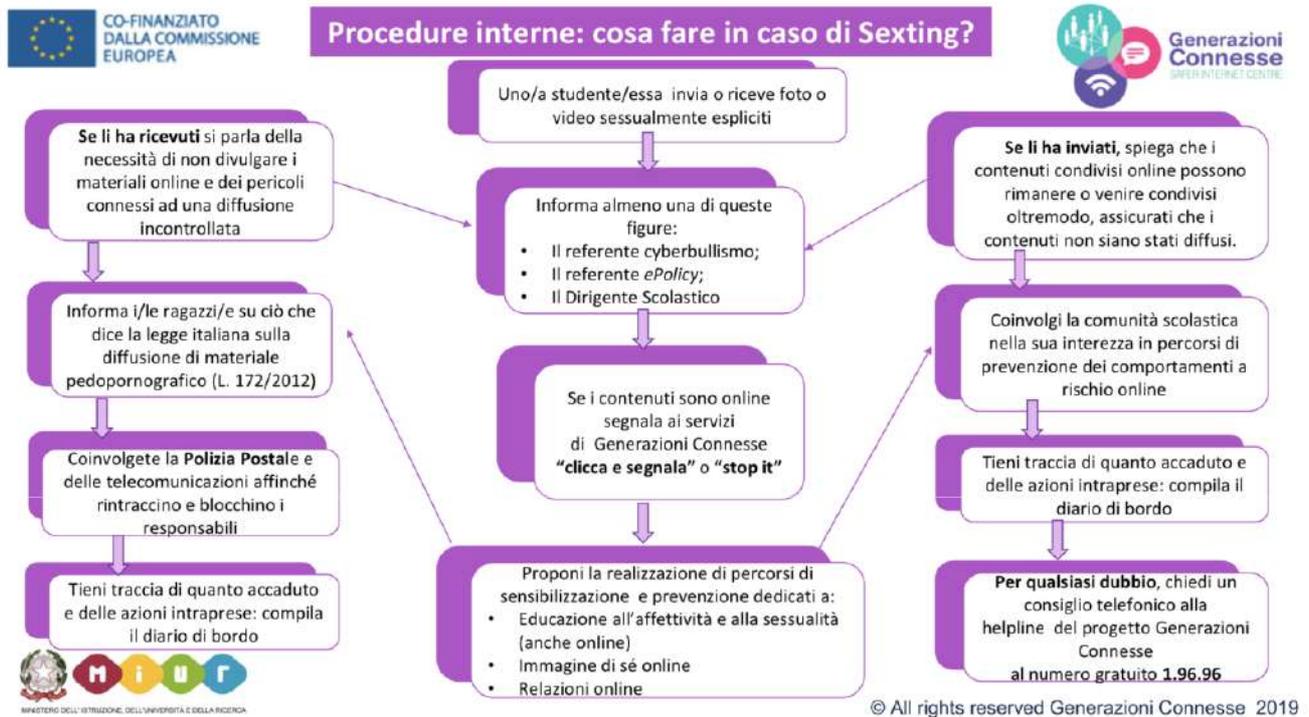
come il Lazio e la Lombardia, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da Internet e alle situazioni di rischio correlate.

5.4. - Allegati con le procedure

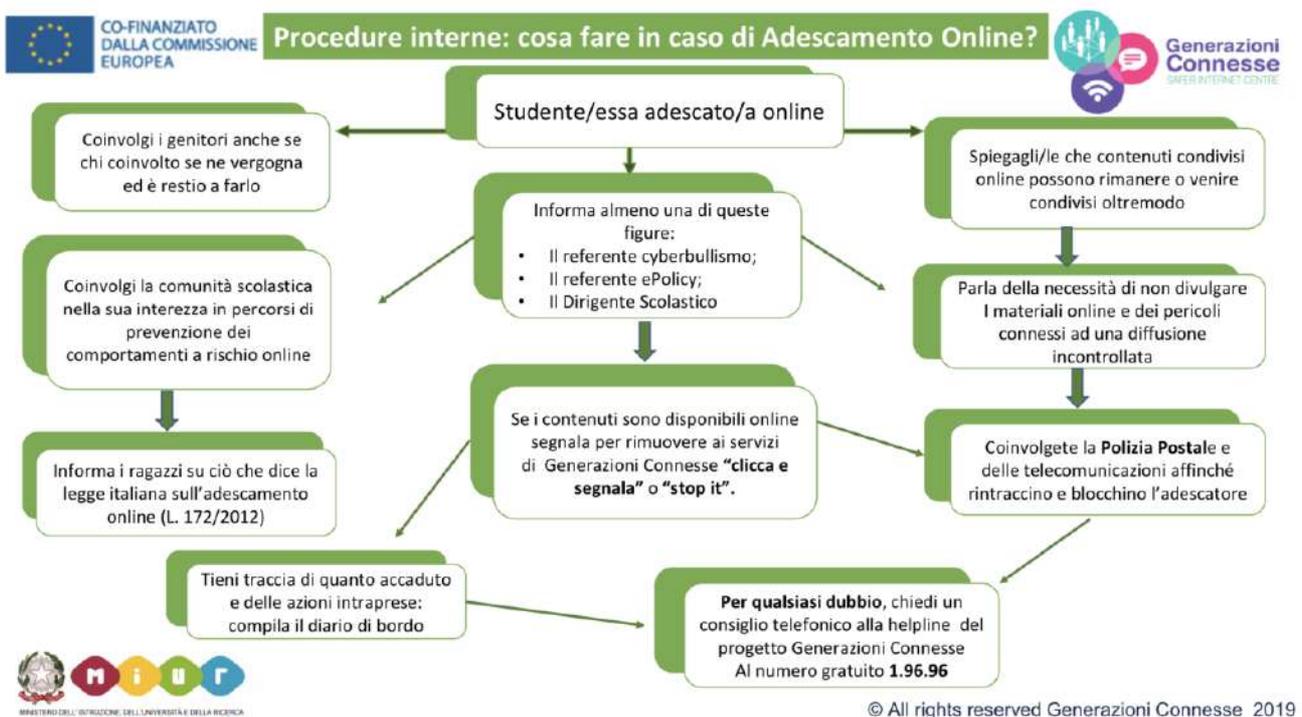
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



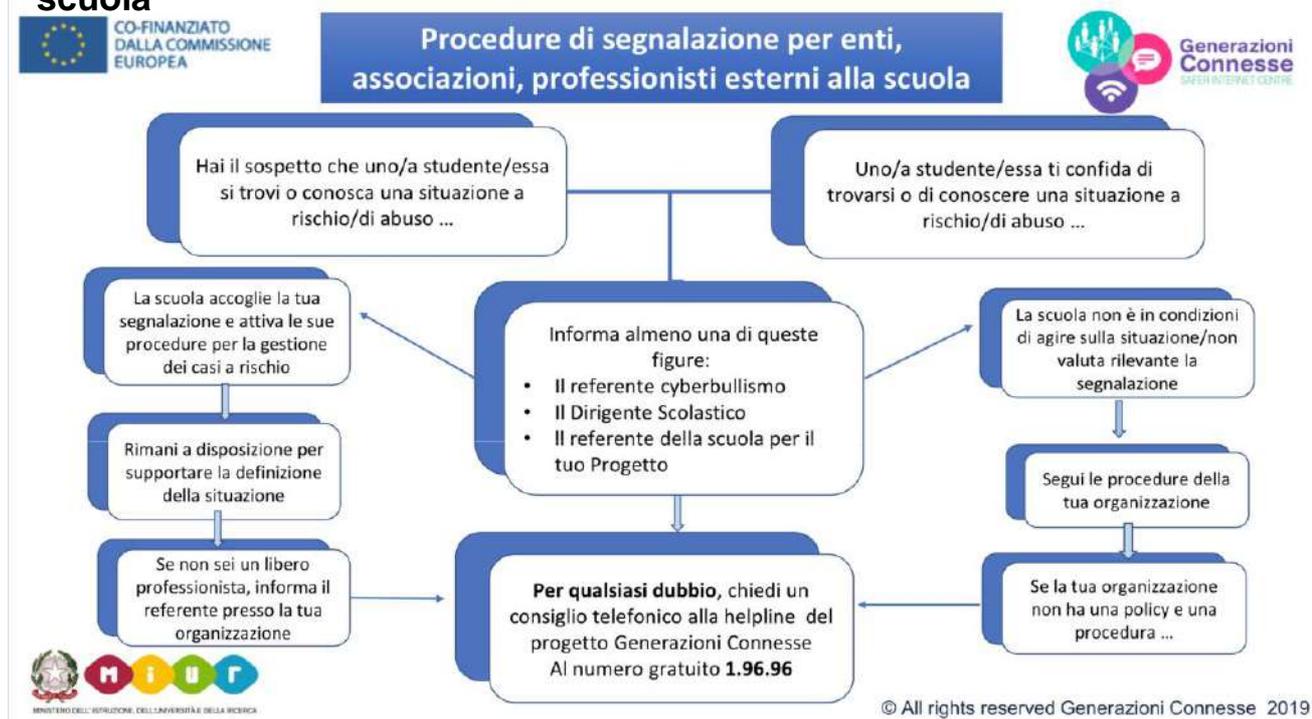
Procedure interne: cosa fare in caso di sexting?



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](#)

MODULO PER IL FOLLOW-UP DEI CASI

Nome di chi compila la segnalazione	Ruolo
_____	_____
Data	Scuola
_____	_____

Descrizione dell'episodio o del problema		
Soggetti coinvolti	Vittima/e: 1..... Classe: 2..... Classe: 3..... Classe:	Autore/autrice e sostenitori: 1..... Classe: 2..... Classe: 3..... Classe:
Chi ha riferito dell'episodio?	- La vittima - Un compagno della vittima, nome: _____ - Genitore, nome: _____ - Insegnante, nome: _____ - Altri, specificare: _____	
Atteggiamento del gruppo	Da quanti compagni è sostenuto il bullo? Quanti compagni supportano la vittima o potrebbero farlo?	
Gli insegnanti sono intervenuti in qualche modo ?		
La famiglia o altri adulti hanno cercato di intervenire ?		
Chi è stato informato della situazione?	<input type="checkbox"/> coordinatore di classe data: <input type="checkbox"/> consiglio di classe data: <input type="checkbox"/> dirigente scolastico data: <input type="checkbox"/> la famiglia della vittima/e data:	<input type="checkbox"/> la famiglia del bullo/i data: <input type="checkbox"/> le forze dell'ordine data: <input type="checkbox"/> altro, specificare: data:

MODULO PER IL FOLLOW-UP DEI CASI

	AZIONI INTRAPRESE	La situazione è
Aggiornamento 1		<input type="checkbox"/> migliorata <input type="checkbox"/> invariata <input type="checkbox"/> peggiorata Come:
Aggiornamento 2		<input type="checkbox"/> migliorata <input type="checkbox"/> invariata <input type="checkbox"/> peggiorata Come:
Aggiornamento 3		<input type="checkbox"/> migliorata <input type="checkbox"/> invariata <input type="checkbox"/> peggiorata Come:
Aggiornamento 4		<input type="checkbox"/> migliorata <input type="checkbox"/> invariata <input type="checkbox"/> peggiorata Come:
Aggiornamento 5		<input type="checkbox"/> migliorata <input type="checkbox"/> invariata <input type="checkbox"/> peggiorata Come:

ALLEGATO B

SCHEDA DI RILEVAZIONE DI ATTI DI BULLISMO E CYBERBULLISMO TRA I RAGAZZI

1. Hai subito delle prepotenze da ragazzi/ragazze a scuola in questi ultimi tre mesi?

- Mai successo in questo periodo
- Una o due volte
- Poche volte
- Diverse volte
- spesso

2. Se si cosa è successo? (anche più risposte)

- Mi hanno dato pugni, calci o spinte in modo continuativo
 - Hanno minacciato di farmi qualcosa di spiacevole
 - Hanno rovinato di proposito delle mie cose personali (abbigliamento, zaino, quaderno, libro, ...)
 - Mi hanno obbligato a dare loro dei soldi
 - Mi hanno derubato
 - Mi hanno offeso pesantemente con parolacce o prese in giro umilianti
 - Hanno messo in giro storie false e bugie su di me
 - Mi hanno escluso dal gruppo per ferirmi
 - Mi hanno obbligato a fare qualcosa di umiliante
 - Ho subito altri tipi di prepotenze (specifica quali nelle righe sotto)
-
-

3. Coloro che hanno messo in atto queste prepotenze

- Sono della mia classe
- Sono di altre classi
- Sia della mia che di altre

4. Ti sei mai reso responsabile di prepotenze verso qualcuno?

- Mai
- Qualche volta
- Spesso
- Mai, però ho assistito a prepotenze verso altri

5. Negli ultimi tre mesi, hai subito offese, molestie o minacce da parte di qualcuno attraverso internet, cellulare o altro mezzo digitale? (fuori dalla scuola)

- Non è mai successo in questo periodo
- È successo una o due volte
- È successo poche volte
- È successo diverse volte
- È successo spesso

6. Cosa ti è successo? (anche più risposte)

- Mi hanno inviato dei messaggi volgari, offensivi o minacciosi
- Hanno pubblicato on-line dei segreti che avevo confidato, per danneggiare i miei rapporti di amicizia o la mia reputazione
- Hanno scritto di me cose non vere, falsità, inventate di proposito per danneggiarmi
- Hanno postato, pubblicato, fotografie o video imbarazzanti/umilianti che mi ritraevano
- Mi hanno escluso per dispetto da un gruppo on-line(chat, social, community)
- Qualcuno ha creato un falso profilo su di me, su una chat o social network
- Ho subito altri tipi di prepotenze(specifica nelle riga sotto)

7. Sempre in questi ultimi mesi, sai se è accaduto qualcosa attraverso internet, chat o social che hanno fatto star male qualcuno che conosci? Scrivi che cosa è accaduto nelle righe sotto:

ALLEGATO C
DIARIO DI BORDO

Schema riepilogativo delle situazioni gestite legate a rischi online

Riepilogo casi							
Scuola _____				Anno Scolastico _____			
N°	Data	ora	Episodio (riassunto)	Azioni intraprese		Insegnante con cui l'alunno/a si è confidato	Firma
				Cosa?	Da chi?		

Il nostro piano d'azioni

Non è prevista nessuna azione.