ISTITUTO di ISTRUZIONE SUPERIORE
"Pertini - Santoni" CROTONE

VIALE MATTEOTTI - 88900 - CROTONE C.F. 81007850795 - C.M KRIS00900G - email: kris00900g@istruzione.it
email pec: kris00900g@pec.istruzione.it - tel. 0962 1888020 - fax 0962 21783021 cell. 3298971190

# E-Safety Policy

**a.s 2020/2021**

**BOZZA**

**PROPOSTA A TUTTA LA COMUNITÀ SCOLASTICA**

**( studenti, genitori, docenti e personale ata)**

Generazioni Connesse
SAFER INTERNET CENTRE

**a cura della Commissione**
**Bullismo e Cyberbullismo**

**INDICE RAGIONATO**

**1. PRESENTAZIONE DELL'EPOLICY**

1.1 Scopo dell'ePolicy
1.2. Ruoli e responsabilità
1.3. Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto
1.4. Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica
1.5. Gestione delle infrazioni alla ePolicy
1.6. Integrazione dell'ePolicy con regolamenti esistenti
1.7. Monitoraggio dell'implementazione dell'ePolicy e suo aggiornamento

2. **FORMAZIONE E CURRICOLO**

2.1 Curricolo sulle competenze digitali per gli studenti.
2.2 Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica.
2.3 Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali
2.4 Sensibilizzazione delle famiglie.

3. **GESTIONE DELL'INFRASTRUTTURA E DELLA STRUMENTAZIONE TIC DELLA E NELLA SCUOLA**

3.1 Protezione dei dati personali
3.2 Accesso ad Internet
3.3 Strumenti di comunicazione online
3.4 Strumentazione personale

**4. RISCHI ON LINE: CONOSCERE, PREVENIRE E RILEVARE**

1. Sensibilizzazione e prevenzione
2. Cyberbullismo: che cos'è e come prevenirlo
3. Hate speech: che cos'è e come prevenirlo
4. Dipendenza da Internet e gioco online
5. Sexting
6. Adescamento online
7. Pedopornografia

**5. SEGNALAZIONE E GESTIONE DEI CASI**

1. Cosa segnalare
2. Come segnalare: quali strumenti e a chi
3. Gli attori sul territorio per intervenire
4. Allegati con le procedure

## 1. PRESENTAZIONE DELL'ePOLICY

L'Istituto ha elaborato questo documento programma anche in conformità con le Linee di Orientamento per azioni di prevenzione e di contrasto al bullismo e cyberbullismo (emanate nell'aprile del 2015 e aggiornate nell' ottobre del 2017) elaborate dal Ministero dell'Istruzione, dell'Università e della Ricerca in collaborazione con il Safer Internet Center per l'Italia, programma comunitario istituito dal Parlamento Europeo e dal Consiglio dell'Unione. Il dettato normativo attribuisce a una pluralità di soggetti compiti e responsabilità ben precisi, ribadendo il ruolo centrale della Scuola che è chiamata a realizzare azioni in un'ottica di governance diretta dal MIUR che includano "la formazione del personale, la partecipazione di un proprio referente per ogni autonomia scolastica, la promozione di un ruolo attivo degli studenti, nonché di ex studenti che abbiano già operato all'interno dell'istituto scolastico in attività di peer education, la previsione di misure di sostegno e di rieducazione dei minori coinvolti"(Art. 4, comma. 2 della Legge n. 71 del 29 maggio 2017).

Come suggerito dalle Linee di Orientamento per la prevenzione e il contrasto del cyberbullismo, c*entrale risulta la figura del docente referente che la scuola individua preferibilmente tra i docenti che posseggano competenze specifiche ed abbiano manifestato l'interesse ad avviare un percorso di formazione specifico. Il referente diventa, così, l'interfaccia con le forze di Polizia, con i servizi minorili dell'amministrazione della Giustizia, le associazioni e i centri di aggregazione giovanile sul territorio, per il coordinamento delle iniziative di prevenzione e contrasto del cyberbullismo.*

Successivamente, per promuovere strategie finalizzate a rendere Internet un luogo più sicuro per gli utenti più giovani, favorendone un uso positivo e consapevole, il MIUR ha avviato l'iniziativa "Generazioni Connesse", cui l'Istituto ha aderito, sostenuta dalla Commissione Europea, con lo scopo di fornire alle istituzioni scolastiche una serie di strumenti didattici, di immediato utilizzo, tra cui:

- attività di formazione (online e in presenza) rivolte in maniera specifica alle comunità scolastiche (insegnanti, ragazzi/e, genitori, educatori) attraverso un percorso dedicato;

- attività di informazione e sensibilizzazione realizzate in collaborazione con la Polizia di Stato per approfondire i temi della navigazione sicura in Rete.

Attraverso un iter guidato e materiali specifici di lavoro, le scuole iscritte a Generazioni connesse, hanno intrapreso un percorso, per far emergere i punti di forza e di debolezza e che consente, all'istituto stesso, di identificare i propri bisogni, le aree di miglioramento e le azioni da intraprendere per giungere all'elaborazione di un progetto personalizzato denominato "Piano d'azione".

Tale Piano consente alle istituzioni scolastiche di focalizzare il proprio Piano Triennale dell'Offerta Formativa al fine di definire:

- il proprio approccio alle tematiche legate alle competenze digitali, alla sicurezza online e ad un uso positivo delle tecnologie digitali nella didattica;

- le norme comportamentali e le procedure per l'utilizzo delle tecnologie dell'informazione e della comunicazione (ICT) in ambiente scolastico;

- le misure per la prevenzione;

- le misure per la rilevazione e gestione delle problematiche connesse a un uso non consapevole delle tecnologie digitali.

Per la realizzazione del "Piano d'azione", l'istituto scolastico è affiancato da un servizio di "supporto scuole" (supportoscuole@generazioniconnesse.it) e da personale qualificato del Safer Internet Centre - Italia.

Un ulteriore strumento per contrastare comportamenti dannosi online e allo stesso tempo accrescere la conoscenza del fenomeno è "iGloss@ 1.110 , l'Abc dei comportamenti devianti online", elaborato dal Dipartimento per la Giustizia Minorile e di Comunità. Il glossario, nella ricognizione dei termini specialistici sui comportamenti online a rischio, offre una sintetica spiegazione delle principali caratteristiche delle condotte devianti e dei risvolti socio-giuridici. L'obiettivo non è esclusivamente descrivere e inquadrare i nuovi fenomeni della devianza online, ma favorire, altresì, l'acquisizione di consapevolezza sulle conseguenze sociali e giudiziarie di queste specifiche trasgressioni.

La Legge 71/2017, ovvero la Legge Ferrara, indica per la prima volta tempi e modalità per richiedere la rimozione di contenuti ritenuti dannosi per i minori. Il documento è diviso in 4 paragrafi uno dei quali norma le Modalità di segnalazione di situazioni e comportamenti a rischio.

La legge definisce il bullismo come *aggressione o molestia ripetuta, allo scopo di ingenerare timore, ansia, isolamento ed emarginazione* e, l'art.1., Comma 2**,** definisce il cyberbullismo come *"Qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti online aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo"*

Oggi la tecnologia consente ai bulli di infiltrarsi nelle case delle vittime, di materializzarsi in ogni momento della loro vita, perseguitandole con messaggi, immagini, video offensivi inviati tramite smartphone o pubblicati sui siti web tramite Internet. Il bullismo diventa

quindi cyberbullismo. Il cyberbullismo definisce un insieme di azioni aggressive e intenzionali, di una singola persona o di un gruppo, realizzate mediante strumenti elettronici (sms, mms, foto, video, e-mail, chat rooms, istant messaging, siti web, telefonate), il cui obiettivo è quello di provocare danni ad un coetaneo incapace a difendersi.

I punti fondamentali della legge che sono stati approfonditi dalla comissione:

- La possibilità di chiedere l'oscuramento, il blocco o la rimozione di tutti i dati relativi al minore vittima di cyberbullismo e, se necessario, di rivolgersi al Garante per la protezione dei dati personali, per ottenere la rimozione entro 48 ore.
- L'attivazione, da parte del Questore, della procedura di ammonimento nei riguardi del minore responsabile di atti di cyberbullismo, verso altri minori, per i quali non sia stata ancora proposta denuncia.
- Il totale coinvolgimento, ad ogni livello, del mondo della scuola, nell'educazione all'uso consapevole della rete ed al contrasto del cyberbullismo.
- L'istituzione di un tavolo interministeriale permanente, coordinato dal MIUR, per la prevenzione ed il monitoraggio del fenomeno.
- L'individuazione, in ogni Istituto scolastico, di un docente referente, che coordina le iniziative di prevenzione e di lotta al cyberbullismo.

La Legge 71/2017 si presenta con un approccio inclusivo e invita a sviluppare una progettualità volta alla prevenzione e al contrasto del bullismo e del cyberbullismo, secondo una prospettiva di intervento educativo e mai punitivo, prevedendo, tra l'altro, all'art.3, di redigere un piano di azione integrato e realizzare un sistema di raccolta di dati per il monitoraggio.

In Calabria, come in altre regioni di Italia, mancano studi sistematici su tale fenomeno che coinvolge, in primis, la scuola; difatti, quasi tutte le ricerche, sono state condotte, generalmente, senza un adeguato piano di campionamento. Il nostro Istituto ha proceduto, pertanto, attraverso la somministrazione di questionari, creati ad hoc dalla commissione bullismo e cyberbullismo, ad un'indagine approfondita che fosse di grande utilità per la realizzazione di interventi finalizzati a prevenire e contrastare il fenomeno, prendendo come riferimento le indagini di altre regioni e relativi Osservatori.

Ogni attore del mondo scuola ritiene Internet una preziosa risorsa per l'educazione e l'informazione ma è pur vero che l'uso sempre più capillare della rete ha esposto gli utenti, e in particolare i minori, e i soggetti con divario digitale, o con limitate competenze informatiche, a nuovi rischi che possono scaturire dalla inadeguata conoscenza dei modi legittimi di usare la rete e dalla scarsa consapevolezza delle stesse funzioni.

L'obiettivo della nostra scuola è quello di educare e sensibilizzare gli adolescenti, gli insegnanti e i genitori all'uso sicuro e consapevole di internet.

Per la stesura del documento, il Gruppo di lavoro, ha fatto riferimento a tutti i materiali messi a disposizione del sito Generazioni Connesse e ha tenuto conto delle EPolicy, pubblicate in Rete, di varie Scuole riconosciute come "virtuose".

## 1.1 Scopo della Policy

Lo scopo della e-Safety Policy è di condividere e stabilire con tutti i membri della comunità scolastica regole, modalità e principi sull'utilizzo consapevole e corretto di internet. In particolare, essa viene redatta per regolare il comportamento della componente studentesca dentro le aule scolastiche e di tutta la comunità educante per sensibilizzarli all'adozione di buone pratiche anche fuori dalla scuola.

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.

Parimenti è fondamentale la formazione degli insegnanti. Studi recenti suggeriscono che gli insegnanti hanno un ruolo importante per rilevare le problematiche di cyberbullismo nella scuola ed intervenire in modo efficace. La letteratura evidenzia come i docenti che si sono formati su questi temi e che partecipano attivamente a progetti di prevenzione, si percepiscano come più efficaci e sicuri nella gestione di problematiche relative al bullismo e al cyberbullismo, siano più attenti ai vissuti delle vittime e si sentano più sicuri nell'affrontare incidenti e situazioni di emergenza a scuola e con le famiglie. Inoltre, nelle classi dove i docenti si sentono più efficaci e capaci di rispondere e gestire i conflitti tra gli studenti, si registra un più basso livello di bullismo e cyberbullismo.

La scuola opererà in stretto collegamento con le forze dell'ordine e con le istituzioni del settore educativo, per mettere in campo strategie di prevenzione al cyber bullismo e interventi di recupero nel caso in cui vengano individuati tali fenomeni, informando i genitori/tutori e chiedendo la loro collaborazione anche qualora gli episodi si siano verificati al di fuori delle attività didattiche.

Le indicazioni, contenute nella presente e-Safety Policy, intendono dare, al nostro Istituto, un impulso allo sviluppo di una cultura d'uso corretto e consapevole delle tecnologie digitali , sia tramite il richiamo a norme vigenti, sia con l'indicazione di prassi e protocolli operativi, opportuni per un uso sempre più professionale da parte di tutto il personale e per la prevenzione dei rischi e la gestione delle emergenze.

I principi fondamentali richiamati sono:

- salvaguardare e proteggere gli studenti e tutti i membri della comunitaà scolastica;
- assistere il personale della scuola per consentirgli di lavorare in modo sicuro e responsabile con le tecnologie digitali, monitorare i propri standard e le proprie prassi didattiche e di comunicazione interna alla scuola;
- impostare chiare aspettative di comportamento e/o codici di condotta rilevanti per un uso responsabile della rete a scopo didattico, personale o ricreativo;
- adottare un protocollo di intervento per rilevare, monitorare e gestire gli stili di abuso online;
- garantire che tutti i membri della comunità scolastica siano consapevoli del fatto che il comportamento illecito o pericoloso dell'utilizzo della rete comporta adeguate azioni disciplinari e giudiziarie.

Relativamente all'uso delle tecnologie digitali e della rete, la scuola:

- promuove l'uso, consapevole e critico,
- fa acquisire procedure e competenze proprie dei mezzi ma anche corrette norme comportamentali,
- previene, rileva e fronteggia le eventuali problematiche che derivano da un utilizzo non responsabile, pericoloso o dannoso,
- promuove l'adozione di strategie che limitino l'accesso a siti e/o applicazioni illeciti.

Appena il caso di sottolineare che è compito degli insegnanti guidare gli studenti nelle attività online a scuola e indicare regole di condotta chiare per un uso critico e consapevole della Rete anche a casa, per prevenire il verificarsi di situazioni potenzialmente pericolose.

La presente policy sarà parte integrante del Regolamento di Istituto e sarà resa nota agli operatori e gli utenti della scuola; si intende, infatti, attivare e mantenere nella nostra scuola una eSafety Policy, in materia di tecnologie dell'informazione e della comunicazione condivisa e accettata da tutti.

Il nostro Istituto, in sintesi, 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 al suo uso.

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

### 1.2 Ruoli e Responsabilità

| | |
|---|---|
| **1. Dirigente scolastico**<br><br>Il ruolo del Dirigente scolastico nel promuovere l'uso consentito delle tecnologie e di internet include i seguenti compiti: | I dirigenti scolastici sono chiamati a effettuare misure di intervento immediato qualora vengano a conoscenza di episodi di cyber bullismo e dovranno essere integrate e previste nei Regolamenti di Istituto e nei Patti di Corresponsabilità;<br>- Sarà cura del dirigente assicurare alle famiglie la massima informazione di tutte le attività e iniziative intraprese, anche attraverso una sezione dedicata sul sito web della scuola, che potrà rimandare al sito del MIUR www.generazioniconnesse.it ;<br>- è auspicabile che il dirigente scolastico attivi specifiche intese con i servizi territoriali (servizi della salute, servizi sociali, forze dell'ordine, servizi minorili dell'amministrazione della Giustizia) in grado di fornire supporto specializzato e continuativo ai minori coinvolti ove la scuola non disponga di adeguate risorse;<br>- garantire che tutti gli insegnanti ricevano una formazione adeguata a svolgere efficacemente l'insegnamento volto a promuovere una cultura dell'inclusione, del rispetto dell'altro/a e delle differenze, un utilizzo positivo e responsabile delle Tecnologie dell'Informazione e della comunicazione (TIC);<br>- condividere e seguire le procedure previste dalle norme in caso di reclami o attribuzione di responsabilità al personale scolastico in relazione a incidenti occorsi agli alunni nell'utilizzo delle TIC a scuola.<br>- A tale scopo necessita di ricevere tempestive informazioni sulle violazioni al presente regolamento o eventuali problemi di cui può venire a conoscenza il corpo docente o il personale ATA . |

| | |
|---|---|
| **2.Animatore digitale** | Il Piano Nazionale Scuola Digitale del 27 ottobre 2015 parla e introduce questa figura di sistema che contribuisce a supportare azioni del Piano, ma anche attività didattiche nelle scuole e tanto altro.<br>Accompagnati dalle funzioni strumentali per le tecnologie, gli AD dovrebbero, secondo il Piano e i decreti ministeriali, avere diverse funzioni e portare avanti l'innovazione digitale nel mondo scolastico.<br>**I riferimenti normativi sono:**<br>LEGGE 107/2015<br>PNSD<br>DM MIUR 16 GIUGNO 2015 n. 435<br>DM n. 851 del 27/10/2015<br>Nota Prot. n° 17791 del 19/11/2015<br>DDG DGEFID n. 50<br>L'AD è un docente di ruolo individuato dall'Istituzione scolastica che affianca il DS e il DSGA nella progettazione e realizzazione dei progetti di innovazione digitale contenuti nel PNSD. Una sola persona, interna alla scuola, non un esperto esterno, che collabori alla diffusione di iniziative innovative.<br><br>**Compiti**<br>Il PNSD e i diversi decreti stabiliscono i compiti di queste figure all'interno della scuola per una durata triennale, salvo eventuali proroghe. Tra i compiti c'è sicuramente conoscere il Piano Nazionale Scuola Digitale e sviluppare progetti relativi alle sue azioni da inserire nel PTOF, su 3 ambiti:<br>formazione interna, coinvolgimento della comunità scolastica, creazione di soluzioni innovative. I tre punti focali del suo lavoro, secondo il DD n. 50 del 2015, sono:<br>**la Formazione interna**: stimolare la formazione interna alla scuola negli ambiti del PNSD attraverso l'organizzazione di corsi on line o in presenza, come formatore o come organizzatore della formazione, favorendo la partecipazione della comunità scolastica sia ai laboratori interni alla scuola che a quelli organizzati dagli snodi formativi e dagli ambiti; |

| | |
|---|---|
| | il **Coinvolgimento della comunità scolastica**: "favorire la partecipazione e stimolare il protagonismo degli studenti nell'organizzazione di workshop e altre attività, anche strutturate, sui temi del PNSD, anche attraverso momenti formativi aperti alle famiglie e ad altri attori del territorio, per la realizzazione di una cultura digitale condivisa";<br>la **Creazione di soluzioni innovative**: "individuare soluzioni metodologiche e tecnologiche sostenibili da diffondere all'interno degli ambienti della scuola (es. uso di particolari strumenti per la didattica di cui la scuola si è dotata; la pratica di una metodologia comune; informazione su innovazioni esistenti in altre scuole; un laboratorio di coding per tutti gli studenti), coerenti con l'analisi dei fabbisogni della scuola stessa, anche in sinergia con attività di assistenza tecnica condotta da altre figure".<br>L'AD dovrebbe coordinarsi con le funzioni strumentali della scuola, con gli animatori del territorio e con gli esperti esterni per contribuire alla realizzazione degli obiettivi previsti.<br>Tra i suoi compiti le fonti parlano di "trasferire le competenze e diffondere le buone pratiche; rendere le scuole autonome nella gestione delle tecnologie; ridurre i costi di manutenzione dei laboratori; favorire condizioni per una replica delle esperienze dalla classe alla scuola".<br>Ad ogni scuola è prevista l'assegnazione di 1.000 euro all'anno, vincolati alle attività dei tre ambiti come coordinamento dell'animatore.<br><br>**<u>PUNTI DI FORZA</u>**<br>ɔro di equipe tra DS, DSGA, Segreteria, Docenti, Enti .; comunicazione più efficace attraverso spazi e erca continua di soluzioni innovative; ottimizzazione ɔnalizzata(in presenza o on-line); attenzione alla ere: abilità nell'uso delle nuove tecnologie e capacità<br><br>L'AD dovrebbe formarsi nell' area progettazione(strumenti), area competenze e contenuti, area formazione e accompagnamento. |

| | |
|---|---|
| | **AREE TEMATICHE OGGETTO DELLE PROPOSTE PROGETTUALI**<br>**AREA PROGETTAZIONE**<br>L'animatore digitale dovrebbe essere promotore delle seguenti azioni:<br>• ambienti di apprendimento per la didattica digitale integrata;<br>• realizzazione/ampliamento di rete, connettività, accessi;<br>• laboratori per la creatività e l'imprenditorialità;<br>• biblioteche scolastiche come ambienti mediali;<br>• coordinamento con le figure di sistema e con gli operatori tecnici;<br>• ammodernamento del sito internet della scuola, anche attraverso l'inserimento in evidenza delle priorità del PNSD;<br>• registri elettronici e archivi cloud;<br>• acquisti e fundraising;<br>• sicurezza dei dati e privacy;<br>• sperimentazione di nuove soluzioni digitali hardware e software.<br>**AREA COMPETENZE E CONTENUTI:**<br>• orientamento per le carriere digitali;<br>• promozione di corsi su economia digitale<br>• cittadinanza digitale;<br>• educazione ai media e ai social network<br>• e-Safety;<br>• qualità dell'informazione, copyright e privacy;<br>• azioni per colmare il divario digitale femminile;<br>• costruzione di curricola digitali e per il digitale;<br>• sviluppo del pensiero computazionale:<br>  • introduzione al coding<br>  • coding unplugged<br>  • robotica educativa<br>• aggiornare il curricolo di tecnologia:<br>  • coding<br>  • robotica educativa |

| | |
|---|---|
| | • making, creatività e manualità;<br>• risorse educative aperte (OER) e costruzione di contenuti digitali;<br>• collaborazione e comunicazione in rete: dalle piattaforme digitali scolastiche alle comunità virtuali di pratica e di ricerca;<br>• ricerca, selezione, organizzazione di informazioni;<br>• coordinamento delle iniziative digitali per l'inclusione;<br>• alternanza scuola lavoro per l'impresa digitale.<br>**AREA FORMAZIONE E ACCOMPAGNAMENTO:**<br>• scenari e processi didattici per l'integrazione del mobile, gli ambienti digitali e l'uso di dispositivi individuali a scuola (BYOD);<br>• sperimentazione e diffusione di metodologie e processi di didattica attiva e collaborativa<br>• modelli di assistenza tecnica;<br>• modelli di lavoro in team e di coinvolgimento della comunità (famiglie, associazioni, ecc.);<br>• creazione di reti e consorzi sul territorio, a livello nazionale e internazionale;<br>• partecipazione a bandi nazionali, europei ed internazionali;<br>• documentazione e gallery del pnsd;<br>• realizzazione di programmi formativi sul digitale a favore di studenti, docenti, famiglie, comunità;<br>• utilizzo dati (anche invalsi, valutazione, costruzione di questionari) e rendicontazione sociale (monitoraggi).<br><br>Al fine di garantire la continuità temporale utile per l'attuazione delle azioni del Piano nazionale per la scuola digitale programmate nell'ambito del Piano triennale dell'offerta formativa, l'animatore digitale è individuato per un periodo di durata triennale, salvo eventuali proroghe. |

| | |
|---|---|
| | Una figura importante nella scuola che, se supportata e formata, può aiutare il processo innovativo-digitale in atto nel mondo dell'istruzione. |
| **3. DSGA** | Il DSGA deve:<br>- assicurare, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per garantire che l'infrastruttura tecnica della scuola sia funzionante, sicura e non aperta a uso improprio o a dannosi attacchi esterni;<br>- garantire il funzionamento dei diversi canali di comunicazione della scuola all'interno della scuola e fra la scuola e le famiglie degli alunni per la notifica di documenti e informazioni del Dirigente scolastico e dell'Animatore digitale nell'ambito dell'utilizzo delle tecnologie digitali e della Rete. |
| **4.Referente prevenz. e contrasto bullismo e cyberbullismo** | **Normativa di riferimento**:<br>• Legge n. 107 del 15 luglio 2015 "Riforma del sistema nazionale di istruzione e formazione e delega per il riordino delle disposizioni legislative vigenti", art. 1, commi 7, 57, 58.<br>• Legge n. 71 del 29 maggio 2017 "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo".<br>• "Linee di orientamento per la prevenzione e il contrasto del cyberbullismo"<br>Nell'ambito di ogni istituzione scolastica deve essere nominato, tra tutti i docenti, un **referente scolastico per il cyberbullismo**. In genere si tratta di insegnanti che hanno competenze adatte al ruolo da ricoprire. Nello specifico, secondo l' Art. 4 comma 3 della Legge n. 71 del 2017, il referente deve:<br>• Coordinare le iniziative di prevenzione e di contrasto del cyberbullismo, con l'eventuale collaborazione delle Forze di polizia, Servizi minorili dell'amministrazione della Giustizia, delle associazioni e dei centri di aggregazione giovanili del territorio; |

| | |
|---|---|
| | • Supportare il Dirigente Scolastico nella revisione e stesura di Regolamenti d'Istituto, atti e documenti;<br>• Raccogliere e diffondere le buone pratiche educative, organizzative e azioni di monitoraggio;<br>• Collaborare per la realizzazione di un modello di e-policy d'Istituto;<br>• segnalare tempestivamente situazioni di rischio online o casi di bullismo o cyberbullismo;<br><br>Oltre ai compiti suddetti, il referente deve anche collaborare con il dirigente scolastico nella stesura del Piano Triennale dell'Offerta Formativa (PTOF) e del Patto di Corresponsabilità (D.P.R. 235/07), relativamente alla parte dedicata alle misure per la prevenzione del cyberbullismo. Infine, per quanto riguarda la nomina del referente, la normativa non specifica chi deve individuare tale figura, rimettendo tale scelta all'autonomia delle scuole.<br><br>**PIATTAFORMA ELISA**<br><br>Il ruolo della scuola nel contrasto al cyberbullismo è fondamentale e non può prescindere dall'adeguata formazione dei docenti. Proprio per questo, il MIUR si è impegnato nell'attuazione di un piano nazionale di formazione dei docenti referenti nelle scuole. La formazione avviene tramite la piattaforma ELISA, all'interno della quale è possibile intraprendere un percorso formativo rivolto ai docenti referenti per l'acquisizione delle competenze psico-pedagogiche e sociali per la prevenzione del disagio giovanile. La piattaforma, lanciata a partire dall'a.s. 2018/2019 con nota 4146 del 08-10-2018, prevede due azioni specifiche che non richiedono oneri economici per i partecipanti: la Formazione E-Learning e il Monitoraggio |

| | |
|---|---|
| | **Formazione E-learning**<br><br>La sezione e-learning si articola in 4 corsi, divisi in più moduli per un totale di 25 ore di formazione. I corso sono suddivisi nei seguenti argomenti:<br>• Corso 1: definizione e caratteristiche del bullismo e del cyberbullismo;<br>• Corso 2: fattori di rischio e conseguenze del bullismo e del cyberbullismo;<br>• Corso 3: azioni per prevenire e contrastare tali fenomeni;<br>• Corso 4: strumenti operativi su come valutare e monitorare i fenomeni;<br><br>**Monitoraggio**<br><br>Il sistema di monitoraggio online si rivolge a tutte le scuole italiane e prevede la compilazione periodica di sondaggi online rivolti a studenti, docenti e dirigenti, finalizzati alla definizione di un report personalizzato per il proprio istituto. Il sistema di monitoraggio online ha molteplici funzioni. Innanzitutto, permette di condurre approfondimenti su larga scala per valutare l'incidenza, la prevalenza e l'andamento dei fenomeni di bullismo e cyberbullismo nelle scuole italiane, cogliendo anche quelle situazioni che hanno bisogno di risorse e intervento.<br><br>**ISCRIZIONE ALLA PIATTAFORMA**<br><br>L'iscrizione prevede la compilazione da parte del referente di un modulo da compilare e inviare successivamente alla e-mail della piattaforma. Inoltre, in riferimento alla nota MIUR n. 4920 del 7/11/2019, al fine di potenziare le possibilità d'intervento nell'ambito del contrasto e della prevenzione di tali fenomeni, a partire dall'a.s. 2019/20 è possibile costituire all'interno degli istituti dei gruppi di lavoro attivi. Questa introduzione ha parzialmente modificato la normativa precedente introducendo due importante novità: |

| | |
|---|---|
| | • Ogni istituto scolastico può nominare più di un docente referente (nel modulo di iscrizione si prevede infatti la figura del Docente referente e del Docente del gruppo di lavoro);<br>• La formazione e-learning è aperta anche ad altri docenti (fino ad un massimo di tre per ciascuna scuola) oltre al docente referente.<br>Il referente può:<br>- avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio;<br>- assicurare che l'educazione alla sicurezza online sia incorporata in tutto il programma di studi;<br>- promuovere la consapevolezza e l'impegno per la salvaguardia online in tutta la comunità scolastica;<br>- promuovere la formazione e dare consulenza a tutto il personale;<br>- promuovere attività o progetti da svolgere nelle classi;<br>- applicare e controllare i protocolli di rilevazione, monitoraggio e gestione delle potenziali azioni di cyber bullismo<br>- diffondere la E-Safety Policy attraverso prodotti multimediali e schede semplificative;<br>- collaborare con tutte le agenzie educative e istituzionali<br>(associazioni sportive, polizia postale, associazioni di sostegno, etc.) per prevenire e gestire i casi di possibile cyber bullismo;<br>- coinvolgere la comunità scolastica (alunni, genitori e altri attori del territorio) nella partecipazione ad attività e progetti attinenti all'utilizzo consapevole dei mezzi digitali;<br>- collaborare in team con altre figure scolastiche (Animatore Digitale e Team per l'Innovazione; Referente BES/Inclusione; Referente per la Dispersione);<br>- supportare i Consigli di Classe ed i Coordinatori;<br>suggerire, incentivare e supportare progetti di Istituto relativi allo sviluppo nei discenti delle Competenze |

| | |
|---|---|
| | di Cittadinanza e Costituzione, nonché progetti di prevenzione ed informazione/formazione dell'intera comunità scolastica;<br>- coinvolgere gli altri soggetti della comunità scolastica, con particolare attenzione agli studenti/ex studenti (peer education);<br>- attivare uno Sportello anonimo di segnalazione. |
| **5.Personale scolastico**<br>(ata, segreterie, etc.) | - essere consapevoli dei problemi di sicurezza on-line connessi con l'uso di telefoni cellulari, fotocamere e dispositivi portatili;<br>- comprendere e contribuire a promuovere politiche di e-sicurezza ;<br>- monitorare l'uso di dispositivi tecnologici e attuare politiche scolastiche per quanto riguarda questi dispositivi;<br>- segnalare qualsiasi abuso, anche sospetto, o problema alla Dirigente e ai responsabili della sicurezza online;<br>- usare comportamenti sicuri, responsabili e professionali nel l'uso della tecnologia; garantire che le comunicazioni digitali con gli studenti siano sempre a livello professionale e si svolgano solo attraverso i sistemi scolastici, non attraverso meccanismi personali, per esempio -mail, telefoni cellulari, ecc.<br>- aver letto, compreso e sottoscritto la presente policy; |
| **6. I Docenti**<br>Il ruolo del personale docente e di ogni figura educativa che lo affianca include i seguenti compiti: | - informarsi/aggiornarsi sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di internet e sulla politica di sicurezza adottata dalla scuola, rispettandone il regolamento;<br>- garantire che le modalità di utilizzo corretto e sicuro delle TIC e di internet siano integrate nel curriculum di studio e nelle attività didattiche ed educative delle classi;<br>- garantire che gli alunni capiscano e seguano le regole per prevenire e contrastare l'utilizzo scorretto e pericoloso delle TIC e di internet;<br>- assicurare che gli alunni abbiano una buona comprensione delle opportunità di ricerca offerte |

| | |
|---|---|
| | dalle tecnologie digitali e dalla rete ma anche della necessità di evitare il plagio e di rispettare la normativa sul diritto d'autore;<br>- garantire che le comunicazioni digitali dei docenti con alunni e genitori siano svolte nel rispetto del codice di comportamento professionale ed effettuate con sistemi scolastici ufficiali ,quindi non private<br>- evitare partecipazione a gruppi di condivisione di whatsapp o altro, inerenti alla scuola ( gruppi classe, gruppi genitori, etc..), se non autorizzati dalla Dirigente;<br>- assicurare la riservatezza dei dati personali trattati ai sensi della normativa vigente;<br>- segnalare al Dirigente scolastico, al vicario del Dirigente scolastico e al referente sul bullismo, qualsiasi abuso, anche solo sospetto, rilevato a scuola nei confronti degli alunni in relazione all'utilizzo delle tecnologie digitali o di internet, per l'adozione delle procedure previste dai protocolli qui adottati;<br>- Gli insegnanti sono responsabili delle TIC nell'ambito dell'attività didattica e hanno il compito di responsabilizzare gli alunni per divenire consapevoli dell'importanza della salvaguardia di un bene comune, seguendo le corrette norme di utilizzo.<br>- controllare l'uso delle tecnologie digitali, dispositivi mobili, macchine fotografiche, ecc. da parte degli alunni durante le lezioni e ogni altra attività scolastica (ove consentito);<br>- nelle lezioni in cui è programmato l'utilizzo di Internet, guidare gli alunni a siti controllati e verificati come adatti per il loro uso e controllare che nelle ricerche su Internet siano trovati e trattati solo materiali idonei;<br>- comunicare al referente sul bullismo e alla Dirigente scolastica, bisogni o disagi espressi dagli alunni(ovvero valutazioni sulla condotta non adeguata degli stessi) rilevati a scuola e connessi all'utilizzo delle TIC, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo;<br>- presenza di un docente o di un adulto responsabile |

| | |
|---|---|
| | durante l'utilizzo di Internet, della piattaforma o di altre TIC, da parte dei ragazzi;<br>- attenzione all'utilizzo di penne USB, CD/DVD o altri dispositivi esterni personali e dell'istituto;<br>- dare chiare indicazioni sul corretto utilizzo della rete (Internet, piattaforma studenti ecc.), condividendo con gli alunni la netiquette e indicandone le regole;<br>- non divulgare le credenziali di accesso agli account (username e password) e/o, nel caso ne sia a conoscenza, alla rete wifi;<br>- non allontanarsi dalla postazione lasciandola incustodita, se non prima di aver effettuato la disconnessione;<br>- non salvare sulla memoria locale della postazione di classe file contenenti dati personali e/o sensibili;<br>- proporre agli alunni attività di ricerca di informazioni in rete fornendo opportunamente loro indirizzi dei siti e/o parole chiave per la ricerca cui fare riferimento.<br>- illustrare ai propri alunni le regole di utilizzo contenute nel presente documento;<br>- aver letto, compreso e sottoscritto la presente policy; |
| **7. Gli Alunni** | - essere responsabili, in relazione al proprio grado di maturità e di apprendimento, per l'utilizzo dei sistemi delle tecnologie digitali in conformità con quanto richiesto dai docenti;<br>- avere una buona comprensione delle potenzialità offerte dalle TIC per la ricerca di contenuti e materiali ma anche della necessità di evitare il plagio e rispettare i diritti d'autore;<br>- comprendere l'importanza di adottare buone pratiche di sicurezza on-line quando si utilizzano le tecnologie digitali per non correre rischi;<br>- adottare condotte rispettose degli altri anche quando si comunica in rete;<br>- esprimere domande, difficoltà o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o di internet ai docenti e ai genitori.<br>- leggere, comprendere, ed accettare la eSafety policy |

| | |
|---|---|
| | - capire l'importanza di segnalare abusi, o l'uso improprio o l'accesso a materiali inappropriati;<br>- sapere quali azioni intraprendere se loro o qualcuno che conoscono si sente preoccupato o vulnerabile quando si utilizza la tecnologia on-line;<br>- conoscere e capire la politica relativa all'uso dei telefoni cellulari, fotocamere digitali dispositivi portatili;<br>- conoscere e capire la politica della scuola sull' uso di immagini e il cyberbullismo;<br>- capire l'importanza di adottare buone pratiche di sicurezza on-line quando si usano le tecnologie digitali fuori dalla scuola;<br>- assumersi la responsabilità di conoscere i benefici e i rischi di utilizzo di Internet e di altre tecnologie in modo sicuro, sia a scuola che a casa.<br>- non utilizzare propri dispositivi esterni personali senza aver acquisito il permesso da parte dell'insegnante;<br>- chiudere correttamente la propria sessione di lavoro.<br>- utilizzare le TIC, SOLO, su indicazioni del docente;<br>- accedere all'ambiente di lavoro con il corretto account (per gli alunni delle classi per le quali è stato attivato un account Google apps for education), non divulgandone le credenziali di accesso (username, password), e archiviare i propri documenti in maniera ordinata e facilmente rintracciabile nella cartella riferita alla classe in cui è presente;<br>- non manomettere le impostazioni dei PC della scuola;<br>- comprendere l'importanza della segnalazione di ogni abuso, uso improprio, o accesso a materiali inappropriati, e conoscere il protocollo per tali segnalazioni;<br>- essere consapevoli del significato e della gravità di atti di cyberbullismo, a tutela della propria e altrui incolumità, al fine di evitare di perpetrare violazioni al Regolamento d'Istituto ed al Patto di Corresponsabilità o, nei casi più gravi, reati punibili da parte della Magistratura;<br>- assumersi la responsabilità di un eventuale utilizzo sbagliato delle tecnologie. |

| | |
|---|---|
| | Gli alunni possono portare il dispositivo (smartphone) a scuola. Secondo con quanto indicato dalla Direttiva Ministeriale n. 30 del 15 marzo 2007, dall'accordo BYOD POLICY, e dal Garante sulla Privacy, gli studenti devono tenere il dispositivo (smartphone) spento quando sono a scuola, indipendentemente dall'attività svolta (lezione, ricreazione, accesso ai servizi igienici, pause, ecc.). Tuttavia, se il docente lo ritiene opportuno, è consentito l'uso del dispositivo personale dello studente che quindi utilizzerà esclusivamente la rete scolastica. Si recepisce in questo documento quanto previsto dalla Direttiva Ministeriale n. 30 del 15 marzo 2007: "le famiglie si assumono l'impegno di rispondere direttamente dell'operato dei propri figli nel caso in cui, ad esempio, gli stessi arrechino danni ad altre persone". |
| **8. I Genitori** | - Sostenere e condividere la linea di condotta della scuola adottata nei confronti dell'utilizzo delle tecnologie dell'Informazione e delle Comunicazioni nella didattica;<br>- Seguire gli alunni nello studio a casa adottando i suggerimenti e le condizioni d'uso delle TIC indicate dai docenti, in particolare controllare l'utilizzo del pc e di internet;<br>- Concordare con i docenti linee di intervento coerenti e di carattere educativo in relazione ai problemi rilevati per un uso non responsabile o pericoloso delle tecnologie digitali o di internet;<br>- Fissare delle regole per l'utilizzo del computer e tenere sotto controllo l'uso che i figli fanno di internet e del telefonino in generale.<br>- Sostenere la scuola nel promuovere la sicurezza online e approvare la e-policy,<br>- Per comunicazioni inerenti alla scuola, utilizzare un linguaggio appropriato e nel rispetto di tutti. |

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

Tutti gli attori che entrano in relazione educativa con gli studenti e le studentesse devono:

- mantenere sempre un elevato profilo personale e professionale, eliminando atteggiamenti inappropriati, essere guidati dal principio di interesse superiore del minore, ascoltare e prendere in seria considerazione le opinioni ed i desideri dei minori, soprattutto se preoccupati o allertati per qualcosa.

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

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

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.

### 1.4 Condivisione e comunicazione della policy all'intera comunità scolastica

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

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

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

Il documento viene esposto in versione semplificata negli spazi che dispongono di pc collegati alla Rete o comunque esposto in vari punti spaziali dell'Istituto. Successivamente si condividerà nelle seguenti modalità, a seconda degli attori interessati, per raggiungere in modo più incisivo le singole parti:

**alunni:**

- Attraverso la discussione in classe della policy nei primi giorni di scuola, con particolare riguardo al protocollo di utilizzo di internet per le nuove classi prime;
- Attraverso l'inserimento di un estratto di questo documento nel diario scolastico e in particolare dei comportamenti da attuare in caso di bisogno.
- Istruzione e informazione riguardo l'uso responsabile e sicuro di internet; questa fase dovrà precedere l'accesso alla rete;
- Comunicazione scritta dell'elenco delle regole per la sicurezza on-line che sarà affissa in tutte le aule o laboratori con accesso a internet;
- Promozione di eventi e/o dibattiti informativi e formativi, in momenti diversi dell'anno, rivolti a tutto il personale, agli alunni e ai loro genitori, con il coinvolgimento di esperti, sui temi oggetto del Documento.
- Tra le misure di prevenzione che la scuola metterà in atto ci saranno, inoltre, azioni finalizzate a promuovere una cultura dell'inclusione, del rispetto dell'altro e delle differenze, così che, l'utilizzo di Internet e dei cellulari, oltre che collocarci all'interno di un sistema di relazioni, ci renda consapevoli di gestire, con un certo grado di trasparenza, i rapporti che si sviluppano in tale ambiente, giungendo a riconoscere e gestire le proprie emozioni. A tal proposito si potrà attivare uno "Sportello di ascolto" rivolto a tutti gli alunni, articolato in colloqui individuali e/o collettivi, al fine di migliorare il benessere personale e scolastico mediante un'attività di supporto della sfera emotiva, relazionale e comportamentale. Si prevede al suo interno, anche uno spazio riservato ai docenti e genitori al fine di individuare strategie efficaci per affrontare problematiche tipiche dell'età adolescenziale.

**personale:**

La linea di condotta della scuola in materia di sicurezza nell'utilizzo delle tecnologie digitali e di internet sarà comunicata formalmente a tutto il personale con il presente documento e altro materiale informativo anche sul sito web.

Tutto il personale è consapevole che una condotta non in linea con il codice di comportamento dei pubblici dipendenti e i propri doveri professionali è sanzionabile.

**genitori** :

- L'attenzione dei genitori sulla sicurezza nell'uso delle tecnologie digitali e di internet sarà attirata nelle news o in altre aree del sito web della scuola;
- Sarà incoraggiato un approccio di collaborazione nel perseguimento della sicurezza nell'uso delle TIC e di internet in occasione degli incontri scuola-famiglia, assembleari, collegiali e individuali;
- La scuola fornirà ai genitori suggerimenti e indicazioni per l'uso sicuro delle tecnologie digitali e di internet anche a casa;

- I docenti di classe forniranno ai genitori indirizzi sul web relativi a risorse utili per lo studio e a siti idonei per gli alunni funzionalmente alle attività didattiche progettate;
- Organizzazione di incontri di sensibilizzazione sul tema della sicurezza informatica e di informazione circa i comportamenti da monitorare o da evitare.
- Allo scopo di condividere regole comuni per l'utilizzo sicuro di Internet sia a casa che a scuola, tutti i genitori saranno invitati a prestare la massima attenzione a principi e regole contenute nel presente documento.

**1.5 Gestione delle infrazioni alla e Policy**

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.

**Mancanze disciplinari**

Tutte le infrazioni andranno tempestivamente segnalate al Dirigente Scolastico, che avrà cura di convocare le parti interessate onde valutare le possibili azioni da intraprendere.
La Scuola prenderà e manterrà nel tempo tutte le precauzioni necessarie e adatte per garantire agli studenti l'accesso a materiale e ambienti appropriati, anche se è impossibile evitare in assoluto che essi trovino materiale indesiderato navigando su un computer della scuola. La scuola non può farsi carico della responsabilità per il materiale trovato in Rete o per eventuali conseguenze causate dall'accesso ad Internet.
Il Referente per il bullismo e il suo Team sono coloro ai quali bisogna rivolgersi immediatamente nel caso in cui si verifichino incidenti o comportamenti dubbi.
Qualsiasi sospetto, rischio o violazione va segnalato immediatamente al Referente che riferisce al Dirigente. Al personale, agli studenti e agli altri componenti della comunità scolastica sono date informazioni sulle infrazioni previste e le eventuali sanzioni.
Le sanzioni riferite soprattutto agli alunni avranno come carattere preferenziale quello educativo/riabilitativo e in ogni caso verrà coinvolta la componente genitori, in qualità di primi educatori. All'interno del Regolamento d'Istituto si trovano invece le diverse sanzioni, graduate in modo proporzionale rispetto alla gravità delle varie forme di bullismo. E' fondamentale per l'Istituto, anche nella sanzione, creare sempre occasioni di recupero. Risulta infatti possibile commutare i giorni di sospensione con attività socialmente utili alla comunità scolastica o alle associazioni convenzionate.

**Mancanze disciplinari nel caso di atti di bullismo o cyberbullismo**

Non tutte le situazioni conflittuali possono essere considerate Bullismo ma, per poter connotare un comportamento come tale dobbiamo osservare se sono presenti tali elementi:
l'intenzionalità: il bullo agisce intenzionalmente al fine di acquisire vantaggi di varia natura, siano essi materiali o gratificazione personale;
la pianificazione: il bullo non colpisce a caso ma pianifica metodo ed azioni scegliendo la vittima;
la persistenza nel tempo:il bullo reitera le azioni nel tempo, per settimane, mesi o anni;

l’asimmetria nella relazione: il bullo, percependosi come essere superiore, sceglie la vittima che, isolata, vive in uno stato di impotenza e di impossibilità di fuga dalla situazione vissuta.

**Differenze tra cyberbullismo e bullismo tradizionale**

- l'anonimato: il bullo utilizzando account falsi si sente al sicuro convinto di non poter essere individuato;

- assenza di relazione tra vittima e bullo: difficilmente la vittima individua il suo persecutore se non chiede aiuto agli adulti di riferimento;

- mancanza di feedback emotivo: il cyberbullo, non percepisce la sofferenza provocata annullando qualunque senso di responsabilità;

- spettatori infiniti: poiché ciò che viene immesso in rete raggiunge potenzialmente tutti ed è “per sempre”, la platea si amplia all’infinito.

Sono da considerarsi tipologie persecutorie qualificate come BULLISMO:

- La violenza fisica o psicologica o l’intimidazione operata dal singolo o dal gruppo, specie se reiterata, con l’intenzione di nuocere e l’isolamento della vittima.

Sono da considerarsi tipologie persecutorie qualificate come CYBERBULLISMO:

- FLAMING: litigi on line nei quali si fa uso di un linguaggio violento e volgare
- HARASSMENT: molestie attuate attraverso l’invio ripetuto di messaggi offensivi
- CYBERSTALKING: invio ripetuto di messaggi contenenti esplicite minacce fisiche o fortemente intimidatori, al punto che la vittima arriva a temere per la propria incolumità
- DENIGRAZIONE: pubblicazione all’interno di comunità virtuali di pettegolezzi, commenti denigratori, dicerie crudeli o foto compromettenti per danneggiare la reputazione della vittima
- EXPOSURE: pubblicazione on line di segreti, informazioni private e/o imbarazzanti su un’altra persona
- IMPERSONIFICAZIONE: sostituzione di persona con l’obiettivo di inviare messaggi ingiuriosi che screditano la vittima; violazione dell’account di qualcuno per farsi passare per questa persona ed inviare messaggi per dare una cattiva immagine della stessa e danneggiarne la reputazione
- ESCLUSIONE: escludere deliberatamente una persona da un gruppo on line (come una lista di amici) per ferirla
- OUTING AND TRICKERY: carpire la fiducia della vittima e rendere pubblici, o minacciare di farlo, i materiali e le informazioni di cui si viene in possesso

- CYBERBASHING O HAPPY SLAPPING: pubblicazione e condivisione online di atti violenti, registrati durante l'aggressione a sconosciuti.

**Indicazioni operative**

Una prima indicazione da tener presente per intervenire efficacemente in queste situazioni è capire se si tratta effettivamente di *cyberbullismo* o di altra tipologia di comportamenti disfunzionali. Oltre al contesto, altri elementi utili ad effettuare questa valutazione sono le modalità in cui avvengono (alla presenza di un "pubblico"? Tra coetanei? In modo cronico e intenzionale? etc.) e l'età dei protagonisti.
Si parla infatti di *cyberbullismo* solo se le persone coinvolte sono minorenni.
Una seconda indicazione operativa concerne una valutazione circa l'eventuale stato di disagio vissuto dalla/e persona/e minorenne/i coinvolte per cui potrebbe essere necessario rivolgersi ad un servizio deputato ad offrire un supporto psicologico e/o di mediazione.
Le strutture pubbliche a cui rivolgersi sono i servizi socio-sanitari del territorio di appartenenza (ad esempio: spazio adolescenti, se presente, del Consultorio Familiare, servizi di Neuropsichiatria Infantile, centri specializzati sulla valutazione o l'intervento sul bullismo o in generale sul disagio giovanile, i comportamenti a rischio in adolescenza, etc.). Parallelamente, nel caso in cui si ipotizzi che ci si possa trovare di fronte ad una fattispecie di reato (come, ad esempio, il furto di identità o la persistenza di una condotta persecutoria che mette seriamente a rischio il benessere psicofisico del bambino/a o adolescente coinvolto/a in qualità di vittima) si potrà far riferimento agli uffici preposti delle Forze di Polizia per inoltrare la segnalazione o denuncia/querela e permettere alle autorità competenti l'approfondimento della situazione da un punto di vista investigativo.
E' in tal senso possibile far riferimento a queste tipologie di uffici: Polizia di Stato – Compartimento di Polizia postale e delle Comunicazioni; Polizia di Stato – Questura o Commissariato di P.S. del territorio di competenza; Arma dei Carabinieri – Comando Provinciale o Stazione del territorio di competenza; Polizia di Stato – Commissariato on line (attraverso il portale http:// www.commissariatodips.it).

**Sanzioni disciplinari - Contravvenzioni**
L'Istituto considera come infrazione grave i comportamenti accertati che si configurano come forme di bullismo e cyberbullismo e li sanziona sulla base di quanto previsto nel Regolamento di Istituto così come integrato dal presente regolamento.
Gli episodi di bullismo/cyberbullismo saranno sanzionati privilegiando sanzioni disciplinari di tipo riparativo, con attività didattiche di riflessione e lavori a vantaggio della comunità scolastica all'interno dell'Istituto.
Il Dirigente scolastico, in caso di constatato episodio di cyberbullismo, contatterà, comunque, la polizia postale che potrà indagare e rimuovere, su autorizzazione dell'autorità giudiziaria, i contenuti offensivi ed illegali presenti in rete.

**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. Tutto ciò che qui non è normato è da considerarsi regolamentato secondo la disciplina generale.

Il presente documento si integra pienamente con obiettivi e contenuti dei seguenti documenti: PTOF, POF, Regolamento interno, Regolamento per l'utilizzo dei laboratori multimediali.

La policy richiede l'integrazione con l'inserimento delle seguenti norme:

Utilizzo del laboratorio di informatica, delle postazioni di lavoro e dell' utilizzo di internet.

**Disposizioni sull'uso del laboratorio**:

1. Le apparecchiature presenti nella scuola sono un patrimonio comune, quindi, vanno utilizzate con il massimo rispetto.
2. I laboratori informatici e le postazioni informatiche dell'istituto possono essere utilizzati esclusivamente per attività di insegnamento, funzionali all'insegnamento e di formazione del personale docente e non docente.
3. Quando un insegnante, da solo o in classe, usufruisce del laboratorio deve obbligatoriamente registrare il proprio nome e l'eventuale classe nell'apposito registro delle presenze di laboratorio, indicando l'orario di ingresso, quello di uscita e motivazione dell'uso delle postazioni informatiche. Questo allo scopo di poter risalire alle cause di eventuali inconvenienti o danneggiamenti e per comprovare l'effettivo utilizzo dell'aula.
4. L'ingresso degli allievi nei laboratori è consentito solo in presenza dell'insegnante.
5. Il docente accompagnatore è responsabile del corretto uso didattico di hardware e software.
6. Nei laboratori è vietato utilizzare CD personali o USB se non dopo opportuno controllo con sistema di antivirus aggiornato.
7. E' vietato cancellare o alterare files-dati presenti sull'hard disk.
8. Il laboratorio non deve mai essere lasciato aperto o incustodito quando nessuno lo utilizza. All'uscita dal laboratorio sarà cura di chi lo ha utilizzato lasciare il mobilio in ordine, le macchine spente correttamente (chiudi sessione…).
9. In caso di malfunzionamento o guasto dei computer bisogna darne tempestiva segnalazione al responsabile del laboratorio.
10. In caso di malfunzionamento non risolvibile dal responsabile di laboratorio si contatterà personalmente o attraverso il Responsabile di laboratorio, il DSGA.
11. Per motivi di manutenzione straordinaria, in caso di guasti o di virus, i PC possono essere formattati senza preavviso. Si consiglia pertanto di salvare i dati importanti su Cd o USB, periodicamente. In caso di formattazione ordinaria ci sarà un preavviso.

**Disposizioni sull'uso dei software**

1. I software installati sono ad esclusivo uso didattico.
2. In base alle leggi che regolano la distribuzione delle licenze, i prodotti software presenti in laboratorio non sono disponibili per il prestito individuale. Nei casi in cui lo fossero in base a precise norme contrattuali i docenti interessati, dopo aver concordato il prestito con il Responsabile di laboratorio, devono compilare l'apposito registro di consegna software custodito in laboratorio.
3. E' fatto divieto di usare software non conforme alle leggi sul copyright. E' cura dell'insegnante-utente di verificarne la conformità. Gli insegnanti possono installare nuovo software sui PC del laboratorio previa autorizzazione scritta del Responsabile di laboratorio. Si raccomanda, quindi, di verificare che il software installato rispetti le leggi sul copyright.
4. È responsabilità degli insegnanti che chiedono al Responsabile di laboratorio di effettuare copie di cd/dvd per uso didattico, di assicurarsi che la copia non infranga le leggi sul copyright in vigore.

**Accesso a internet**

1. L'accesso a Internet è consentito al personale docente e non docente solo ad esclusivo uso didattico e/o di formazione e alle classi accompagnate e sotto la responsabilità di un insegnante;
2. Internet non può essere usato per scopi vietati dalla legislazione vigente;
3. L'utente è direttamente responsabile, civilmente e penalmente, a norma delle vigenti leggi, per l'uso fatto del servizio Internet;
4. E' vietato inserire sui pc connessi in rete programmi contenenti virus, scaricare software non autorizzati da internet, scaricare e installare software senza licenza.

**Norme finali**

Il Responsabile di laboratorio che verifichi un uso del laboratorio contrario a disposizioni di legge o del regolamento interno deve darne comunicazione per iscritto al Dirigente Scolastico.

**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 nostro piano d'azioni**

**Azioni da svolgere entro un'annualità scolastica**:

- Organizzare un evento di presentazione del progetto Generazioni Connesse rivolto agli studenti.
- Organizzare un evento di presentazione del progetto Generazioni Connesse rivolto ai docenti.
- Organizzare un evento di presentazione del progetto Generazioni Connesse rivolto ai genitori.
- Organizzare un evento di presentazione e conoscenza dell'ePolicy rivolto agli studenti.
- Organizzare un evento di presentazione e conoscenza dell'ePolicy rivolto ai docenti.
- Organizzare un evento di presentazione e conoscenza dell'ePolicy rivolto ai genitori.

**Azioni da svolgere nei prossimi 3 anni:**

- Azione 1 (Azione sviluppabile nell'arco di un anno): Formazione del personale docente
- Azione 2 (Azione sviluppabile nell'arco di due anni): Formazione Peer-Education
- (16 alunni delle classi terze)
- Azione 3 (Azione sviluppabile nell'arco di tre anni: Intervento dei Peer-Education nelle classi prime di ogni anno scolastico.
- Azione 4 (Azione sviluppabile nell'arco di tre anni): Incontri con consulenti esterni rivolti agli studenti, genitori, docenti e personale ATA relativamente al contrasto bullismo e cyberbullismo.
- Azione 5 (Azione sviluppabile alla fine di ogni anno scolastico): Restituzione da parte dei Peer-Education del lavoro di formazione svolto nelle classi al Team antibullismo.
- Azione 6 (Azione sviluppabile alla fine di ogni anno scolastico): Restituzione del lavoro svolto da parte del Team al Collegio docenti.

## 2 FORMAZIONE E CURRICOLO

La nostra scuola condivide le linee indicate nel Piano Nazionale Scuola Digitale (PNSD) che danno, come indirizzo, l'intento di modificare gli ambienti di apprendimento per rendere l'offerta formativa coerente con i cambiamenti della società della conoscenza e con le esigenze e gli stili cognitivi delle nuove generazioni. Il D.M. 851 del 27 ottobre 2015, in attuazione dell'art.1, comma 56 della legge 107/2015 è finalizzato a:

- migliorare le competenze digitali degli studenti anche attraverso un uso consapevole delle stesse;
- implementare le dotazioni tecnologiche della scuola al fine di migliorare gli strumenti didattici e laboratoriali ivi presenti;
- favorire la formazione dei docenti sull'uso delle nuove tecnologie ai fini dell'innovazione didattica;
- individuare un Animatore Digitale ed un team per l'innovazione digitale che supporti ed accompagni adeguatamente l'innovazione didattica, nonché l'attività dell'animatore Digitale;
- partecipare a bandi nazionali ed europei per finanziare le suddette iniziative.

### 2.1. Curricolo sulle competenze digitali per gli studenti

I ragazzi usano la Rete quotidianamente, talvolta in modo più "intuitivo" ed "agile" rispetto agli adulti, ma non per questo sono dotati di maggiori "competenze digitali". Infatti, "la competenza digitale presuppone l'interesse per le tecnologie digitali e il loro utilizzo con dimestichezza e spirito critico e responsabile per apprendere, lavorare e partecipare alla società. Essa comprende l'alfabetizzazione informatica e digitale, la comunicazione e la collaborazione, l'alfabetizzazione mediatica, la creazione di contenuti digitali (inclusa la programmazione), la sicurezza (compreso l'essere a proprio agio nel mondo digitale e possedere competenze relative alla cybersicurezza), le questioni legate alla proprietà intellettuale, la risoluzione di problemi e il pensiero critico" ("Raccomandazione del Consiglio europeo relativa alla competenze chiave per l'apprendimento permanente", C189/9, p.9). Per questo la scuola si impegna a portare avanti percorsi volti a promuovere tali competenze, al fine di educare gli studenti e le studentesse verso un uso consapevole e responsabile delle tecnologie digitali. Ciò avverrà attraverso la progettazione e implementazione di un curricolo digitale e una progressiva educazione alla sicurezza online.

Nello specifico si intende :

- promuovere un uso consapevole delle nuove tecnologie;
- sensibilizzare e attivare gli studenti sui rischi e i pericoli derivanti da un uso non corretto dei social network;
- favorire lo sviluppo di una cittadinanza attiva e responsabile;
- educare e sensibilizzare i minori ai rischi associati all'utilizzo di piattaforme di condivisione;
- conoscere e acquisire consapevolezza su natura, ruolo e opportunità delle TSI nel quotidiano;
- distinguere il reale dal virtuale, pur riconoscendone le correlazioni;
- sviluppare le abilità di base nelle TIC (uso del computer per reperire, valutare, conservare, produrre, presentare e scambiare informazioni);

- acquisire consapevolezza su come le TIC possono coadiuvare la creatività e l'innovazione; riflettere sulle problematiche legate alla validità e all'affidabilità delle informazioni disponibili.

In virtù della valenza trasversale delle competenze digitali, la loro acquisizione verrà promossa attraverso percorsi didattici disciplinari e/o interdisciplinari inerenti diverse aree, coerentemente con gli obiettivi individuati nel curricolo di Istituto.

### 2.2 Formazione dei docenti sull'utilizzo e l'integrazione delle TIC 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 professione docente è complessa e pertanto richiede competenze diverse ed integrate, fra queste anche quelle di tipo digitale. Le TIC, infatti, dovrebbero essere usate dagli insegnanti ad integrazione della didattica al fine di progettare, sviluppare, utilizzare, gestire e valutare i processi di insegnamento e apprendimento di tutti gli studenti e le studentesse della classe, anche delle persone con disabilità (in chiave inclusiva). Il PTOF, del nostro Istituto, prevede che una parte della formazione in servizio sia dedicata proprio all'uso e all'inserimento delle TIC nella didattica. Tale formazione è svolta o da docenti dell'Istituto con formazione specifica o organizzando incontri con esperti esterni per permettere una adeguata formazione agli insegnanti stessi. Inoltre, la scuola assicura tempestiva e capillare informazione su corsi, convegni e seminari che riguardino tali argomenti, cercando altresì di agevolare il personale che intenda parteciparvi, con l'obiettivo di una formazione che consenta la revisione delle prassi metodologiche e didattiche adottate e promuova la consapevolezza di un nuovo modo di essere educatori di studenti, oramai, sempre connessi, ma spesso inconsapevoli dei pericoli della Rete e per i quali occorre una preparazione specifica, se si vuole rispondere ai loro nuovi stili cognitivi e comunicativi.

### 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.

Nell'ottica di creare ulteriore sinergia fra scuola, studenti/studentesse e famiglie, di promuovere la condivisione di buone pratiche nell'utilizzo consapevole delle TIC e di prevenire e contrastare ogni forma di discriminazione, offesa, denigrazione e lesione della dignità dell'altro, nonché fenomeni di bullismo e cyberbullismo, è necessario e auspicabile che i docenti tutti dell'Istituto scolastico seguano un percorso formativo specifico ed adeguato che abbia ad oggetto non solo l'uso responsabile e sicuro della Rete ma anche i rischi legati a quest'ultima. Essere docenti formati sulle tematiche in oggetto vuol dire non pensare esclusivamente all'alfabetizzazione ai media ma anche considerare la sfera emotiva e affettiva degli studenti e delle studentesse che usano le nuove tecnologie. Essi/e, infatti, comunicano, esprimono se stessi e sviluppano l'identità personale e sociale, attraverso i dispositivi tecnologici che sempre di più consentono loro di poter entrare in contatto con il mondo che li circonda. Prestare attenzione a questi aspetti significa dare loro gli strumenti per poter educare ragazzi e ragazze alle emozioni in contesto onlife e quindi modulare e gestire i propri ed altrui comportamenti, favorendo e promuovendo forme di convivenza civile.

Si creeranno, a tal fine, momenti formativi di approfondimento (progetti specifici, laboratori, eventi, giornate, etc, ...) con la famiglia e gli/le studenti/studentesse in modo da sensibilizzare l'intera comunità educante sia su un corretto uso delle tecnologie digitali sia sulle potenzialità della Rete. I momenti di formazione e aggiornamento saranno pensati e attuati a partire dall'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica; dall'analisi del fabbisogno conoscitivo circa particolari argomenti che si sentono come più cogenti per i docenti e l'Istituto; dall'analisi delle richieste che provengono dagli studenti e dalle studentesse.

Di seguito, un cronoprogramma che consideri il triennio scolastico, in un'ottica di vera e propria programmazione, con azioni specifiche:

- Analizzare il fabbisogno formativo degli insegnanti sull'uso sicuro della Rete;
- Promuovere la partecipazione dei docenti a corsi di formazione che abbiano ad oggetto i temi del progetto "Generazioni Connesse".
- Monitorare le azioni svolte per mezzo di specifici momenti di valutazione;
- Organizzare incontri con professionisti della scuola o con esperti esterni, enti/associazioni, etc**.**

Il banner del progetto "**Generazioni connesse**" è stato inserito sul sito della scuola, all'interno è possibile trovare approfondimenti, spunti, aggiornamenti e strumenti didattici utili da usare con gli studenti e le studentesse. Nella sezione, saranno messi a disposizione materiali per l'aggiornamento sull'utilizzo consapevole e sicuro di Internet, prevedendo possibilità e modalità di condivisione fra gli insegnanti.

## 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 gli studenti e le studentesse 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, attraverso l'aggiornamento, oltre che del regolamento scolastico, anche del "Patto di corresponsabilità", nonché mettendo a disposizione sul sito web dell'Istituto tutti i materiali e i documenti prodotti dalla scuola in materia di prevenzione del fenomeno del Bullismo e del Cyberbullismo, i riferimenti normativi, la filmografia, i materiali informativi e diversi link a siti di informazione specifica, utili per un maggior approfondimento del fenomeno da parte di studenti e famiglie. Per informare le famiglie sulle condotte che si dovranno adottare a scuola e, in generale, offrire loro consigli da mettere in pratica con i propri figli, il nostro Istituto mette in atto le seguenti azioni :

- **elaborare regole sull'uso delle tecnologie digitali** da parte dei genitori nelle comunicazioni con la scuola e con i docenti (es. mail, gruppo whatsapp, sito della scuola etc.) e informarli adeguatamente anche riguardo alle regole per gli studenti e le studentesse;
- **fornire ai genitori consigli o linee guida sull'uso delle tecnologie digitali nella comunicazione** con i figli e in generale in famiglia
- organizzare percorsi di sensibilizzazione e formazione dei genitori su un uso responsabile e costruttivo della Rete in famiglia e a scuola.
- prevedere azioni e strategie per il coinvolgimento delle famiglie in tali percorsi di sensibilizzazione, ad esempio, mediante l'organizzazione di iniziative in cui anche gli studenti e le studentesse siano protagonisti.

**Il nostro piano d'azioni rivolto ai docenti**

AZIONI (da sviluppare nell'arco dell'anno scolastico 2020/2021)

- Effettuare un'analisi del fabbisogno formativo sull'utilizzo e l'integrazione delle TIC nella didattica.
- Effettuare un'analisi del fabbisogno formativo sull'uso consapevole e sicuro della Rete e delle tecnologie digitali.
- AZIONI (da sviluppare nell'arco dei tre anni scolastici successivi).

- Organizzare e promuovere incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare e promuovere incontri formativi sull'uso consapevole e sicuro di Internet e delle tecnologie digitali.

## 3 GESTIONE DELL'INFRASTRUTTURA, DELLA STRUMENTAZIONE TIC DELLA SCUOLA E DELLA STRUMENTAZIONE PERSONALE

La scuola metterà in atto tutte le azioni necessarie per garantire agli studenti l'accesso alla Rete adottando tutti i sistemi di sicurezza conosciuti per diminuire le possibilità di rischio durante la navigazione. Resta fermo che non è possibile garantire una navigazione totalmente priva di rischi e che la Scuola e gli insegnanti non possono assumersi le responsabilità conseguenti all'accesso accidentale e/o improprio a siti illeciti.

### 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".*

Il 25 maggio 2018 è entrato in vigore in tutti gli stati aderenti all'Unione Europea il Regolamento del Parlamento Europeo 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, conosciuto come GDPR.

Anche se in parte quanto previsto dal nuovo Regolamento risulta facilmente sovrapponibile alla precedente normativa italiana, è però necessario ricordare che il GDPR diventa il nuovo riferimento per garantire la corretta tutela dei dati personali. Pertanto il nostro Istituto adeguerà le modalità e responsabilità opportune a questo documento. Sono dati personali le informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, etc. Garantire la corretta tutela dei dati personali richiede, innanzitutto, l'individuazione dei dati trattati soggetti alla normativa vigente, nonché l'analisi delle modalità e responsabilità di gestione delle informazioni, onde identificare le eventuali criticità e gli adeguamenti da predisporre. Con l'evoluzione delle nuove tecnologie, i dati personali hanno assunto un ruolo significativo, come quelli relativi alle comunicazioni elettroniche (via Internet o telefono) e quelli che consentono la geolocalizzazione, fornendo informazioni sui luoghi

frequentati e sugli spostamenti. La nostra scuola è impegnata in prima persona nella tutela della privacy degli utenti attraverso l'applicazione del regolamento d'Istituto e del patto di corresponsabilità. Particolare attenzione è data, dalla nostra Istituzione, nei confronti degli studenti quando questi sono minorenni, in ottemperanza all'articolo 8 della Carta dei diritti fondamentali dell'Unione europea tutelato dal regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, recepito dal nostro ordinamento dal D.Lgs. 10 agosto 2018 n. 101, entrato in vigore lo scorso 19 settembre 2018. Saranno da individuare le misure di tutela attuate e da definire quelle da attuare, nonché le modalità per garantirne nel tempo la continuità e l'adeguatezza. Dovranno inoltre essere stabilite le responsabilità per la gestione dei dati: titolare, responsabile, persone autorizzate al trattamento. L'I.I.S. Pertini Santoni di Crotone, tratta i dati personali forniti dagli utenti in conformità alla normativa vigente, rispetta la privacy dei propri utenti e si impegna a proteggere i dati personali che gli stessi conferisconoall'istituto stesso. La raccolta ed il trattamento di dati personali avvengono, quando necessari, in relazione all'esecuzione di servizi richiesti dall'utente, o quando l'utente stesso decide di comunicare i propri dati personali; in tali circostanze, la presente politica della privacy illustra le modalità ed i caratteri di raccolta e trattamento dei dati personali dell'utente. In caso di raccolta di dati personali, informerà l'utente sulle finalità della raccolta al momento della stessa, ove necessario, richiederà il consenso dell'utente, non comunicherà i dati personali dell'utente a terzi senza il consenso dello stesso. Se l'utente decide di fornire alla scuola i propri dati personali, la scuola potrà comunicarli all'interno dell'Istituto od a terzi che prestano servizi alla scuola, solo rispetto a coloro che hanno bisogno di conoscerli in ragione delle proprie mansioni, e, ove necessario, con il permesso dell'utente. La scuola tratta i dati personali dell'utente per le seguenti finalità di carattere generale: per soddisfare le richieste a specifici prodotti o servizi, per personalizzare la visita dell'utente al sito, per aggiornare l'utente sulle ultime novità in relazione ai servizi offerti od altre informazioni che ritiene siano di interesse dell'utente che provengono direttamente dall'Istituto o dai suoi partners, e per comprendere meglio i bisogni dell'utente ed offrire allo stesso servizi migliori. Il trattamento di dati personali dell'utente da parte dell'Istituto. per le finalità sopra specificate avviene in conformità alla normativa vigente a tutela dei dati personali. Infine, si fa riferimento a tutto quanto previsto dal Decreto legislativo 30 giugno 2003, n. 196 (c. d. Codice della Privacy).

Tuttavia, si possono individuare al riguardo alcune linee guida di e-safety:

- L'utilizzo di telefoni cellulari, di apparecchi per la registrazione di suoni e immagini, quando autorizzato dai docenti, è consentito, ma esclusivamente per fini personali, e sempre nel rispetto dei diritti e delle libertà fondamentali delle persone coinvolte (siano essi studenti o professori) in particolare della loro immagine e dignità.

Le istituzioni scolastiche hanno, comunque, la possibilità di regolare o di inibire l'utilizzo di registratori, smartphone, tablet e altri dispositivi elettronici all'interno delle aule o nelle scuole stesse. Gli studenti e gli altri membri della comunità scolastica, in ogni caso, non possono diffondere o comunicare sistematicamente i dati di altre persone (ad esempio

pubblicandoli su Internet) senza averle prima informate adeguatamente e averne ottenuto l'esplicito consenso. ( da vademecum privacy del Garante)

- Registrazione delle lezione e strumenti compensativi: È possibile registrare la lezione esclusivamente per scopi personali, ad esempio per motivi di studio individuale. Per ogni altro utilizzo o eventuale diffusione, anche su Internet, è necessario prima informare adeguatamente le persone coinvolte nella registrazione (professori, studenti…) e ottenere il loro esplicito consenso. Nell'ambito dell'autonomia scolastica, gli istituti possono decidere di regolamentare diversamente o anche di inibire l'utilizzo di apparecchi in grado di registrare. In ogni caso deve essere sempre garantito il diritto degli studenti con diagnosi DSA (disturbi specifici dell'apprendimento) o altre specifiche patologie di utilizzare tutti gli strumenti compensativi (come il registratore) di volta in volta previsti nei piani didattici personalizzati che li riguardano. ( da vademecum privacy del Garante)
- È consigliabile utilizzare canali istituzionali per comunicazioni a scopo didattico con le famiglie e gli studenti
- Le fotografie o i video da pubblicare sul sito che includano allieve e allievi saranno selezionati con cura e non permetteranno a singoli di essere chiaramente identificati a meno che non si tratti di eventi particolari per cui le famiglie potranno concedere opportuna autorizzazione. La scuola cercherà di utilizzare fotografie o video di gruppo piuttosto che foto integrali di singoli.
- I nomi completi di alunne e alunni saranno evitati sul sito web come pure nei blog, forum e wiki, in particolare se in associazione con le loro fotografie.
- All'atto dell'iscrizione è richiesto alle famiglie di firmare un'autorizzazione scritta per consentire l'uso didattico di immagini e video delle/dei minori secondo i principi sopra indicati.
- Ogni caso particolare sarà preso in considerazione per stabilire l'opportunità di pubblicare dati personali e sarà presentata apposita richiesta circostanziata che varrà solo per lo specifico evento.

### 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. In ottemperanza a quanto stabilito dall'articolo 2 della Dichiarazione dei diritti di Internet, elaborata dalla Commissione per i diritti e i doveri in Internet, la scuola si è doterà di un software dedicato di controllo di tutti gli accessi in Internet dai dispositivi scolastici e individuerà un docente interno espressamente formato all'uopo.

È vietato l'uso dei dispositivi personali se non espressamente autorizzati dai docenti per fini esclusivamente didattici.

Relativamente all'accesso ad Internet si specifica quanto segue:

1. L'accesso a Internet è consentito al personale docente e non docente solo ad esclusivo uso didattico e/o di formazione e alle classi accompagnate e sotto la responsabilità di un insegnante;
2. Internet non può essere usato per scopi vietati dalla legislazione vigente;
3. L'utente è direttamente responsabile, civilmente e penalmente, a norma delle vigenti leggi, per l'uso fatto del servizio Internet;
4. E' vietato inserire sui pc connessi in rete programmi contenenti virus, scaricare software non autorizzati da internet, scaricare e installare software senza licenza.
5. E' obbligatorio, prima di installare qualsiasi programma , consultare l'animatore digitale, un responsabile di laboratorio o un tecnico per valutarne la compatibilità.

**Linee guida di buona condotta dell'utente e buone pratiche nell'uso della rete**

- Rispettare la legislazione vigente;
- Tutelare la propria privacy, quella degli altri utenti e degli alunni al fine di non divulgare notizie private contenute nelle documentazioni elettroniche cui si ha accesso;
- Rispettare la cosiddetta netiquette (regole condivise che disciplinano il rapportarsi fra utenti della rete, siti, forum, mail e di qualsiasi altro tipo di comunicazione).
- Controllo della validità e dell'origine delle informazioni a cui si accede o che si ricevono;
- Utilizzo di fonti alternative di informazione per proposte comparate;
- Ricerca del nome dell'autore, dell'ultimo aggiornamento del materiale e di altri possibili link al sito;
- Rispetto dei diritti di autore e dei diritti di proprietà intellettuale.

**Gestione accessi**

Accesso docenti
L'Istituto attualmente è dotato di una rete wireless destinata all' utilizzo didattico da parte del corpo docente.
Ai docenti è consentito accedere ad Internet da propri dispositivi utilizzando la rete Wi-Fi dell'Istituto previa richiesta alla Dirigente o al suo vicario. Successivamente, le figure preposte, configurano il pc dell'interessato senza comunicare la password.

Accesso studenti
Il Regolamento di Istituto vieta l'uso del cellulare se non per scopi didattici e previa autorizzazione del docente. In particolare, agli studenti non è consentito accedere ad Internet da propri dispositivi utilizzando la rete Wi-Fi dell'Istituto, se non per scopi didattici.
Durante l'orario scolastico agli alunni non è permesso l'utilizzo della telefonia mobile; è altresì vietato l'uso per scopo personale di tutti gli altri strumenti informatici di proprietà e non dello studente. L'eventuale utilizzo di strumenti informatici di proprietà dello studente durante l'attività didattica deve essere autorizzata dal docente.
Relativamente agli alunni che accedono a Internet durante l'attività didattica sono consentiti la navigazione guidata da parte dell'insegnante e la stesura di documenti collaborativi purché sotto il controllo dell'insegnante e nel caso in cui tale attività faccia parte di un progetto di lavoro precedentemente autorizzato. E' vietato l'accesso alle chat-room pubbliche o non moderate.

## 3.3 Strumenti di comunicazione online

Le tecnologie digitali sono in grado di ridefinire gli ambienti di apprendimento, supportando la comunicazione a scuola e facilitando un approccio sempre più collaborativo. L'uso degli strumenti di comunicazione online a scuola, al fianco di quelli

più tradizionali, ha l'obiettivo di rendere lo scambio comunicativo maggiormente interattivo e orizzontale. Tale uso segue obiettivi e regole precise correlati alle caratteristiche, funzionalità e potenzialità delle tecnologie digitali. Il nostro Istituto, per la comunicazione esterna usa, soprattutto, il sito web della scuola. La scuola offre all'interno del proprio sito una serie di servizi alle famiglie e ai fruitori esterni: i docenti che desiderano pubblicare attività didattiche dovranno chiedere l'autorizzazione al Dirigente**.** Il Dirigente Scolastico e il personale incaricato di gestire le pagine del sito della Scuola hanno la responsabilità di garantire che il contenuto pubblicato sia accurato e appropriato. Come strumenti di comunicazione interna, il nostro Istituto usa il registro elettronico, il servizio di posta elettronica, applicativi e piattaforme di lavoro collaborativo e condiviso. Il registro elettronico permette di gestire la comunicazione con le famiglie, le quali, dopo avere ricevuto le credenziali per l'accesso riservato, possono visualizzare informazioni utili, interagendo con la scuola, relativamente a:

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

La pubblicazione delle informazioni attraverso tale strumento assolve l'obbligo di comunicare prontamente ed efficacemente ogni evento riguardante l'alunno/a.
Docenti e studenti possono utilizzare i servizi di posta elettronica accedendo alla rete della scuola per fini esclusivamente didattici. Studenti e docenti possiedono un account con estensione@pertinikr.edu.it. L'account è strettamente personale, per cui ogni utente dovrà avere cura di disconnettere il proprio accesso al termine del suo utilizzo. Lo spazio è destinato alla ricezione di comunicazioni, all'invio di documentazione e alla condivisione di materiali. Le comunicazioni di posta elettronica, tra personale scolastico, famiglie e allieve/allievi devono avvenire preferibilmente tramite l'account istituzionale o registro elettronico, per consentire l'attivazione di protocolli di controllo.
Un'ultima notazione riguarda i Social network (facebook, whatsapp, instagram, etc..) per alunni, docenti e genitori. Dal punto di vista normativo, l'utilizzo dei Social Network con la pubblicazione di nomi e giudizi sulle persone o sulle istituzioni e la diffusione di foto/filmati senza il consenso e, comunque, all'insaputa delle persone coinvolte può determinare ricadute di carattere anche penale, come ad esempio la diffamazione. Pertanto, rientra nella politica dell'Istituto invitare tutti gli attori della comunità scolastica a non prelevare o diffondere immagini, video registrazioni – anche solo audio – non autorizzate, ed a fare un uso prudente dei Social Network, in particolare Facebook e Whatsapp, limitandone l'uso alle sole comunicazioni funzionali.
Nella pratica didattica si cercherà di educare la componente studentesca al loro uso sicuro.

### 3.4 Strumentazione personale

I dispositivi tecnologici sono parte integrante della vita personale di ciascuno, compresa quella degli/lle studenti/esse e dei docenti (oltre che di tutte le figure professionali che a vario titolo sono inseriti nel mondo della scuola), ed influenzano necessariamente anche la didattica e gli stili di apprendimento. Comprendere il loro utilizzo e le loro potenzialità innovative, diventa di cruciale importanza, anche considerando il quadro di indirizzo normativo esistente e le azioni programmatiche, fra queste il Progetto Generazioni Connesse e il più ampio PNSD. La presente *ePolicy* contiene indicazioni, revisioni o eventuali integrazioni di Regolamenti già esistenti che disciplinano l'uso dei dispositivi personali in classe, a seconda dei vari usi, anche in considerazione dei dieci punti del Miur per l'uso dei dispositivi mobili a scuola (BYOD, "Bring your own device"). Risulta fondamentale per la comunità scolastica aprire un dialogo su questa tematica e riflettere sulle possibilità per l'Istituto di dotarsi di una regolamentazione condivisa e specifica che tratti tali aspetti, considerando aspetti positivi ed eventuali criticità nella e per la didattica. In tal senso, gli smartphone, i tablet e i pc personali possono essere integrati nel lavoro nelle classi quando ben progettato e calibrato per discipline e obiettivi formativi e didattici: si pensi, a titolo di esempio, agli student response systems ossia alla possibilità degli studenti e delle studentesse di rispondere a quiz e sondaggi utilizzando direttamente il proprio smartphone come telecomando sempre sotto la guida e il controllo dell'insegnante.

Di seguito, i dieci i punti del Miur, condivisi dalla nostra scuola, per l'uso dei dispositivi mobili a scuola, BYOD (Bring your own device):

- **Ogni novità comporta cambiamenti.** Ogni cambiamento deve servire per migliorare l'apprendimento e il benessere delle studentesse e degli studenti e più in generale dell'intera comunità scolastica
- **I cambiamenti non vanno rifiutati, ma compresi e utilizzati per il raggiungimento dei propri scopi.**

Bisogna insegnare a usare bene e integrare nella didattica quotidiana i dispositivi anche attraverso una loro regolamentazione. Proibire l'uso dei dispositivi a scuola non è la soluzione. A questo proposito ogni scuola adotta una Politica di Uso Accettabile (PUA) delle tecnologie digitali.

- **La scuola promuove le condizioni strutturali per l'uso delle tecnologie digitali.** Fornisce, per quanto possibile, i necessari servizi e l'indispensabile connettività, favorendo un uso responsabile dei dispositivi personali (BYOD). Le tecnologie digitali sono uno dei modi per sostenere il rinnovamento della scuola.
- **La scuola accoglie e promuove lo sviluppo del digitale nella didattica.** La presenza delle tecnologie digitali costituisce una sfida e un'opportunità per la didattica e per la cultura scolastica. Dirigenti e insegnanti attivi in questi campi sono il motore dell'innovazione. Occorre coinvolgere l'intera comunità scolastica anche attraverso la formazione e lo sviluppo professionale.

- **I dispositivi devono essere un mezzo, non un fine.** È la didattica che guida l'uso competente e responsabile dei dispositivi. Non basta sviluppare le abilità tecniche, ma occorre sostenere lo sviluppo di una capacità critica e creativa.
- **L'uso dei dispositivi promuove l'autonomia delle studentesse e degli studenti.** È in atto una graduale transizione verso situazioni di apprendimento che valorizzano lo spirito d'iniziativa e la responsabilità di studentesse e gli studenti. Bisogna sostenere un approccio consapevole al digitale nonché la capacità d'uso critico delle fonti di informazione, anche in vista di un apprendimento lungo tutto l'arco della vita.
- **Il digitale nella didattica è una scelta: sta ai docenti introdurla e condurla in**
- **classe.** L'uso dei dispositivi in aula, siano essi analogici o digitali, è promosso dai docenti, nei modi e nei tempi che ritengono più opportuni.
- **Il digitale trasforma gli ambienti di apprendimento.** Le possibilità di apprendere sono ampliate, sia per la frequentazione di ambienti digitali e condivisi, sia per l'accesso alle informazioni, e grazie alla connessione continua con la classe. Occorre regolamentare le modalità e i tempi dell'uso e del non uso, anche per imparare a riconoscere e a mantenere separate le dimensioni del privato e del pubblico.
- **Rafforzare la comunità scolastica e l'alleanza educativa con le famiglie.** È necessario che l'alleanza educativa tra scuola e famiglia si estenda alle questioni relative all'uso dei dispositivi personali. Le tecnologie digitali devono essere funzionali a questa collaborazione. Lo scopo condiviso è promuovere la crescita di cittadini autonomi e responsabili.
- **Educare alla cittadinanza digitale è un dovere per la scuola.** Formare i futuri cittadini della società della conoscenza significa educare alla partecipazione responsabile, all'uso critico delle tecnologie, alla consapevolezza e alla costruzione delle proprie competenze in un mondo sempre più connesso.

**Il nostro piano d'azioni**

AZIONI (da sviluppare nell'arco dell'anno scolastico 2020/2021).

- Organizzare uno o più eventi o attività volti a consultare i docenti dell'Istituto per redigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali scuola.

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

- 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 gli studenti e le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity).

## 4 RISCHI ON LINE: CONOSCERE, PREVENIRE E RILEVARE

**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.

### 4.1 SENSIBILIZZAZIONE E PREVENZIONE

L'obiettivo che i docenti della nostra scuola, da tempo, perseguono è operare prevenzione primaria e gestire i fenomeni di violenza di qualsiasi natura, approfondendo e selezionando strategie da attuare innanzi a tali fenomeni. La dinamiche messe in atto creano competenze nei docenti, percepite dagli studenti come protezione e, il processo d'interazione e modulazione reciproco, genera strumenti di trasformazione delle condotte devianti attuate dai giovani alunni. Gli strumenti adottati 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.*

Nello specifico, la nostra offerta formativa:

- Promuovere la conoscenza e la consapevolezza dei problemi connessi al bullismo;
- Mettere in atto azioni per conoscere il vissuto del "bullo", della "vittima" e del contesto:
- Proporre modelli che permettano di indagare ed individuare le dinamiche in essere all'interno del gruppo classe per rappresentarsi la rete relazionale e dunque gli elementi cardine (attraverso l'utilizzo di sociogrammi);
- Facilitare l'acquisizione di tecniche per imparare;

- Promuovere fattori di protezione del singolo e del gruppo: autostima e fiducia in se stessi, capacità d'interazione sociale ed intelligenza emotiva;
- Riconoscere e promuovere fattori di gestione del conflitto nella relazione educativa;
- Proporre modalità operative tra le varie agenzie educative;
- Focalizzare l'attenzione sull'analisi e l'individuazione di situazioni conflittuali.

Le modalità di lavoro sono di tipo esperienziale con l'utilizzo di simulate e di role playing nonché di analisi dei vissuti diretti e indiretti. Vengono usate tecniche quali il modeling e i giochi di gruppo, utilizzando materiale strutturato. Per casi di bullismo sospetto, vengono seguite le linee indicate come specifiche, quali:

- "Approccio senza accusa" (Maines e Robinson)
- "Metodo di interesse condiviso (Pikas)

Le azioni di sensibilizzazione e prevenzione e le modalità messe in atto, offrono agli studenti stimoli per la discussione, il confronto e per le attività di gruppo, favorendo la consapevolezza dei problemi e delle norme di comportamento sia di segno positivo che negativo.

**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".*

Nel rispetto della stessa legge e delle relative Linee di orientamento per la prevenzione e il contrasto del cyberbullismo, che indicano al mondo scolastico ruoli, responsabilità e azioni utili a prevenire e gestire i casi di cyberbullismo, il PTOF del nostro Istituto prevede :

- La formazione del personale scolastico, prevedendo la partecipazione di un proprio referente;
- Lo sviluppo delle competenze digitali, tra gli obiettivi formativi prioritari (L.107/2015);
- La promozione di un ruolo attivo degli studenti (ed ex studenti) in attività di peer education;
- Misure di sostegno e rieducazione dei minori coinvolti;

- L'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;
- Azioni preventive ed educative e non solo sanzionatorie.
- La Nomina del Referente per le iniziative di prevenzione e contrasto che ha il compito di coordinare le iniziative di prevenzione e contrasto del cyberbullismo e che, a tal fine, può avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio. Potrà, inoltre, svolgere un importante compito di supporto al dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d'istituto), atti e documenti (PTOF, PdM, RAV).

### 4.3 - Hate speech: che cos'è e come prevenirlo

La definizione di hate speech è al centro di un ampio dibattito a livello internazionale. Noi nel nostro lavoro abbiamo preso come riferimento quella fornita dalla Raccomandazione di politica generale n. 15 della Commissione europea contro il razzismo e l'intolleranza del Consiglio d'Europa (ECRI) del 21 marzo 2016:

«*L'istigazione, la promozione o l'incitamento alla denigrazione, all'odio o alla diffamazione nei confronti di una persona o di un gruppo di persone, o il fatto di sottoporre a soprusi, molestie, insulti, stereotipi negativi, stigmatizzazione o minacce tale persona o gruppo, e comprende la giustificazione di queste varie forme di espressione, fondata su una serie di motivi, quali la "razza", il colore, la lingua, la religione o le convinzioni, la nazionalità o l'origine nazionale o etnica, nonché l'ascendenza, l'età, la disabilità, il sesso, l'identità di genere, l'orientamento sessuale e ogni altra caratteristica o situazione personale*.» Fonte: www.coe.int/en/web/european-commissionagainst-racism-and-intolerance

Considerando che tale fenomeno, purtroppo, è sempre più diffuso ed estremamente importante affrontarlo anche a livello educativo e scolastico, il nostro Istituto si pone 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.

- Attività che portano a ragionare e interrogarsi sul tema degli stereotipi, andando a scoprire quelli che, anche poco consapevolmente, ognuno mette costantemente

in campo quando vede o conosce una nuova persona. L'obiettivo è quello di ragionare in maniera critica sugli stereotipi, soprattutto sui propri, su quelli che utilizziamo più spesso e in quali circostanze, per una presa di consapevolezza, dopo un'attenta analisi, di quali sono quelli negativi più spesso utilizzati e perché.

- Attività che agevolano spunti di riflessione sui temi del discorso d'odio e del bullismo, e forniscono metodi e strategie per una riflessione critica sulla percezione dei propri compagni riguardo a questi temi. Si lavora su quesiti e dubbi che emergono direttamente da loro, che vengono proposti ai compagni e poi rielaborati in forma grafica.
- Attività per introdurre il tema delle fake news e offrire spunti per ragionare su come le notizie, e il loro metodo di diffusione, possono cambiare la percezione che abbiamo della realtà.

### 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.

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 "craving" (irrefrenabile voglia di utilizzo della Rete). Si tratta di un fenomeno studiato da diversi anni ma la sua individuazione è molto complessa per diverse ragioni. Prima di tutto, non esistono delle norme condivise su cosa definisca uso "eccessivo" (al di là della quantità di tempo trascorso sul web); in secondo luogo, spesso accade che l'utilizzo incontrollato di Internet nasconda altri tipi di dipendenze, rendendo maggiormente complessa la discriminazione della reale problematica.
Ciononostante, i diversi studi analizzati permettono di definire alcuni aspetti utili per fare una prima valutazione di rischio rispetto ad un utilizzo disfunzionale/ patologico della Rete:
a. uso eccessivo – spesso associato ad una perdita del senso del tempo che passa o la dimenticanza di bisogni primari (come, ad esempio, mangiare e dormire);
b. senso di straniamento – con la manifestazione di sentimenti di rabbia, tensione e/o depressione quando il computer o la Rete sono inaccessibili;
c. tolleranza – con il bisogno di accessori sempre migliori per il computer o di un sempre maggiore tempo di utilizzo;
d. ripercussioni negative – incluse discussioni, bugie (soprattutto riguardo al tempo passato online), isolamento sociale e scarsi risultati in ambito scolastico.

La quasi totalità dei ragazzi (89,7%) possiede uno smartphone con l'accesso ad internet e utilizza Whatsapp per rimanere connesso con gli amici - mandando più di 50 messaggi al giorno nel 57,4% dei casi - oppure Facebook (82,3%).

**Indicazioni operative**

Se si ravvisa un rischio per il benessere psicofisico delle persone minorenni sarà opportuno rivolgersi ad un servizio deputato ad offrire un supporto psicologico anche passando per una consultazione presso il medico di base o il pediatra di riferimento. Le strutture pubbliche a cui rivolgersi sono i servizi socio-sanitari del territorio di appartenenza (consultori familiari, servizi di Neuropsichiatria Infantile, i centri specializzati sulle dipendenze, etc.).

Il *videogioco* è un gioco gestito da un dispositivo elettronico che consente di interagire con le immagini di uno schermo. Nato intorno agli anni Cinquanta negli ambienti di ricerca scientifica e nelle facoltà universitarie americane, ha avuto il suo sviluppo a partire dalla seconda metà degli anni Settanta. Come qualsiasi altro gioco, anche il videogioco rappresenta e riproduce differenti contesti e oggetti reali o astratti, temi avveniristici e fantascientifici oppure ispirati al mondo del cinema o della televisione che possono diventare modelli di comportamento per ragazzi e bambini. Per questo motivo, la diffusione dei videogiochi rappresenta un ambito di particolare interesse: il loro utilizzo coinvolge bambini e ragazzi in un processo che si caratterizza in termini di abilità, capacità, maturità che non sono solo tecniche ma legate soprattutto alla capacità dei ragazzi e delle ragazze di elaborare i contenuti a cui sono esposti. C'è un ampio dibattito tra gli esperti e in letteratura sul rapporto tra esposizione ai contenuti violenti veicolati da un videogioco e aumento di comportamenti aggressivi messi in atto da bambini e ragazzi nella vita reale (cfr Dill A., 2000; Clippinger W., 2002 et al). Non si è pervenuti tuttavia a risultati univoci e concordi sull'argomento: differenti studi evidenziano il rischio di una normalizzazione della violenza e la sua imitazione e riproduzione nella vita reale tanto più questa diventa 'normale'. Altri studi ci dicono come i videogiochi non possano essere indicati come le uniche cause di comportamenti violenti nell'età dello sviluppo ma devono piuttosto essere considerati come uno dei tanti fattori che facilitano condotte ostili (cfr Bartolomeo e Caravita, 2004). Identificare le cause e le motivazioni che sono all'origine di atti o atteggiamenti violenti non è infatti semplice. La premessa fondamentale da cui è necessario partire è quindi che i videogiochi non rappresentano di per sè un aspetto problematico e di rischio per lo sviluppo dei bambini/e e/o delle/gli adolescenti. Al contrario, sempre da più parti, e come emerso nel corso della ricerca condotta da Adiconsum *"Il mondo dei videogiochi raccontato dai ragazzi tra falsi miti e opportunità educative"* (2010), si evidenzia un approccio che sottolinea i fattori positivi dei videogiochi: essi sono usati come una risposta ai bisogni di bambini/e e adolescenti inseriti in contesti eterogenei ed interattivi caratterizzati dall'uso coinvolgente e diffuso

delle nuove tecnologie. In tal senso, gli aspetti positivi legati ai videogiochi si riferiscono al fatto che gli stessi possono:

a) contribuire allo sviluppo di abilità tecniche e strategiche;
b) migliorare la coordinazione oculo-motoria;
c) contribuire all'acquisizione di abilità di *problem solving*.

Al tempo stesso le criticità connesse all'utilizzo dei videogiochi da parte dei/lle persone minorenni sono legate alla possibilità di incorrere in alcune problematiche quali:

a) la dipendenza legata ad un loro uso eccessivo;
b) i rischi di violazione della privacy;
c) i contatti indesiderati nei casi di videogiochi online;
d) l'esposizione a contenuti potenzialmente dannosi.

**Indicazioni operative**

E' innanzitutto utile capire se ci troviamo di fronte ad un rischio legato all'uso eccessivo dei videogiochi. Ha senso quindi prestare attenzione nel caso in cui la persona minorenne:

- dedica molto tempo a *videogiocare* (o lo dedicherebbe se non le/gli fosse proibito);
- trascura le altre attività, compresi gli impegni scolastici;
- quando può scegliere, preferisce *videogiocare* piuttosto che passare il tempo con gli amici o fare altro;
- mostra una caduta nel rendimento scolastico;
- mostra un ritiro dalle altre attività sociali;
- gioca di nascosto;
- tende ad essere apatico/a o irascibile quando non può giocare;
- si arrabbia quando lo/la si interrompe mentre gioca, o quando gli/le si impedisce di giocare;
- i pensieri e le fantasie sono focalizzati sul gioco, anche quando svolge altre attività;
- cerca di procurarsi videogiochi sempre nuovi o insiste per averli;
- spende somme considerevoli di denaro (se ne dispone) per i videogiochi;
- presenta alterazioni o anomalie nelle abitudini (alimentazione, igiene personale,
- funzioni fisiologiche, sonno);
- presenta sintomi fisici quali mal di testa, di schiena, dolori al collo, arrossamenti agli occhi, disturbi della vista.

Il nostro istituto è intenzionato a promuovere azioni di prevenzione attraverso percorsi sul benessere digitale.

## 4.5 SEXTING

Il "sexting" è fra i rischi più diffusi connessi ad un uso poco consapevole della Rete. Il termine indica un fenomeno molto frequente fra i giovanissimi che consiste nello scambio di contenuti mediali sessualmente espliciti; i/le ragazzi/e lo fanno senza essere realmente consapevoli di scambiare materiale (pedopornografico) che potrebbe arrivare in mani sbagliate e avere conseguenze impattanti emotivamente per i protagonisti delle immagini, delle foto e dei video. Con il termine *sexting* - dall'inglese, unione di due parole: sex e texting – si fa riferimento allo scambio di immagini o video - in particolare via cellulare - che ritraggono persone minorenni nude, seminude o in atteggiamenti sessuali.

È un fenomeno piuttosto comune tra gli/le adolescenti; si inserisce, infatti, a pieno titolo nel processo di costruzione e scoperta della propria identità ed in particolare della propria sessualità, tipica di questa fase evolutiva. Una foto a seno nudo o sotto la doccia, inviata tramite MMS, diventa, in questo caso, un "regalo" divertente per un fidanzato o una fidanzata; dare/diffondere un'immagine "provocante" di se stessi può rappresentare un modo per dimostrarsi "adulti" o "più maturi" non solo agli occhi degli altri, ma anche verso se stessi e gestire le sfide tipiche dell'età adolescenziale.
A differenza di altri contesti, grazie alle caratteristiche degli strumenti tecnologici, gli adolescenti possono infatti sperimentare e "osare" con più libertà e meno pudori. Questa premessa è utile per dare al fenomeno una lettura obiettiva e capire che, in termini di bisogni a cui fa riferimento, non c'è niente di nuovo.
L'utilizzo delle nuove tecnologie e l'impatto che questo ha sulla modalità in cui il fenomeno si manifesta e nelle conseguenze che alcuni comportamenti possono avere nella vita degli adolescenti coinvolti, richiede invece tutta una serie di riflessioni:

- il *controllo*: quello che si invia tramite cellulare o si posta online è praticamente impossibile da eliminare in forma definitiva; anche se, a pochi istanti dal *click*, ci si pente, qualcuno potrebbe avere già scaricato le immagini dalla pagina internet o averle inoltrate immediatamente ad altre persone. Non solo, il rischio è di esporsi anche a possibili ricatti; chi accede a queste immagini/video, può usarli facilmente per danneggiare volutamente chi è ritratto: un ex partner che vuole vendicarsi? Un cyberbullo? Possono diffondere questo materiale con estrema facilità e le vittime non avranno mai la possibilità di eliminarlo in modo definitivo;
- la *reputazione*: immagini troppo spinte o provocanti, possono nuocere alla reputazione di chi è ritratto, creare problemi con nuovi partner, o addirittura influenzare i futuri rapporti di lavoro;
- *adescamento da parte di adulti potenziali abusanti*: dando una certa immagine di sé online, magari sul profilo di un social network, si possono attirare persone interessate sessualmente a minori che potrebbero essere incentivate ad accedere ai loro dati personali o a tentare un adescamento;
- *pedopornografia*: queste immagini/video rientrano a pieno titolo nella definizione di materiale pedopornografico. Produrre questo materiale e soprattutto diffonderlo è reato, come previsto nel nostro codice penale.

Le implicazioni per le persone minorenni coinvolte dipendono da vari fattori, tra cui l'età (se inferiore ai quattordici anni, il/la minore che ad esempio trattiene e/o diffonde le immagini - non è imputabile) e il livello di consapevolezza rispetto all'azione compiuta. Sebbene le stime europee indichino un calo del fenomeno a livello europeo (nel 2010 la media era il 12%), il sexting rimane un fenomeno molto diffuso.
Di frequente i ragazzi non sono consapevoli delle conseguenze di questi gesti e possono non rendersi conto dei pericoli che comporta l'invio di foto o video, in particolare a persone estranee. Alla base di tali gesti troviamo spesso un profondo senso di sofferenza e solitudine.

**Indicazioni operative**
Nel caso in cui immagini e/o video anche prodotte autonomamente da persone minorenni, sfuggano il loro controllo e vengano diffuse senza il loro consenso è opportuno rivolgersi al più vicino Compartimento di Polizia Postale e delle Comunicazioni con l'obiettivo di ottenere la rimozione del materiale, per quanto possibile, se online e il blocco della sua diffusione via dispositivi mobili.

## 4.6 - Adescamento online

Il ***grooming*** (dall'inglese "groom" - curare, prendersi cura) rappresenta una tecnica di manipolazione psicologica che gli adulti potenziali abusanti utilizzano per indurre i bambini/e o adolescenti a superare le resistenze emotive e instaurare una relazione intima e/o sessualizzata. Gli adulti interessati sessualmente a bambini/e e adolescenti utilizzano spesso anche gli strumenti messi a disposizione dalla Rete per entrare in contatto con loro. I luoghi virtuali in cui si sviluppano più frequentemente tali dinamiche sono le chat, anche quelle interne ai giochi online, i social network in generale, le varie app di instant messaging (whatsapp, telegram etc.), i siti e le app di ***teen dating*** (siti di incontri per adolescenti). Un'eventuale relazione sessuale può avvenire, invece, attraverso webcam o live streaming e portare anche ad incontri dal vivo. In questi casi si parla di adescamento o grooming online. In Italia l'adescamento si configura come reato dal 2012 (art. 609-undecies – l'adescamento di minorenni) quando è stata ratificata la Convenzione di Lanzarote (legge 172 del 1° ottobre 2012); nel testo della Convenzione il reato viene definito come "qualsiasi atto volto a carpire la fiducia di un minore di anni sedici per scopi sessuali, attraverso artifici, lusinghe o minacce posti in essere anche mediante internet o altre reti o mezzi di comunicazione". È importante specificare che il reato si configura anche se l'incontro offline con il minore non avviene, pertanto il reato sussiste anche se l'adescamento non va a buon fine; è sufficiente il tentativo.

**Indicazioni operative**

Se si ritiene di trovarsi di fronte ad una possibile situazione di adescamento online che coinvolge un/a bambino/a o adolescente sarà opportuno che il computer utilizzato dalla persona minorenne non venga più toccato (ad esempio: non sostituirsi al bambino/a e/o adolescente, non rispondere al suo posto, etc.). Contestualmente, sarà opportuno rivolgersi al Compartimento di Polizia Postale e delle Comunicazioni più vicino o ad altro presidio di Polizia (Questura, Commissariati di Polizia di Stato o Caserme dei Carabinieri).

Parallelamente, se si ravvisa un rischio per il benessere psicofisico delle persone minorenni coinvolte sarà opportuno rivolgersi ad un servizio deputato ad offrire un supporto psicologico anche passando per una consultazione presso il medico di base o il pediatra di riferimento. Le strutture pubbliche a cui rivolgersi sono i servizi socio-sanitari del territorio di appartenenza (Consultori Familiari, servizi di Neuropsichiatria infantile, centri specializzati sull'abuso e il maltrattamento all'infanzia, etc.), tenendo comunque in considerazione che l'attuale normativa (legge 172 del 2012, art. 351 c.p.p.) 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 sommarie informazioni con l'ausilio di una persona esperta in psicologia o psichiatria infantile. A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere per prevenire ed affrontare la delicata problematica dell'adescamento.

**AZIONI (da sviluppare nell'arco dell'anno scolastico 2020/2021)**

- Sensibilizzazione sull'esistenza di individui che usano la rete per instaurare relazioni, virtuali o reali, con minorenni e per indurli alla prostituzione.

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

- Azioni volte al consolidamento e alla promozione dei diritti dei bambini e degli adolescenti
- Organizzare uno o più incontri informativi per una sintetica descrizione delle caratteristiche principali di note esperienze significative
- Azioni volte a promuovere l'interculturalità.

**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 esiste almeno da quando esiste la fotografia e, quindi, da prima dell'avvento di internet. Tuttavia, l'espansione senza precedenti delle comunicazioni avvenuta con la Rete, ha radicalmente cambiato il modo in cui il materiale pedopornografico viene prodotto e diffuso, contribuendo ad un aumento della sua disponibilità e accessibilità. Chiunque sia in possesso di competenze informatiche di base è, oggi, in grado di pubblicare o cercare materiale online con relativa facilità, mantenendo un certo livello di anonimato. La diffusione della banda larga consente di caricare e scaricare velocemente video e foto anche di grandi dimensioni, così come la diffusione delle videocamere e dei cellulari con videocamera incorporata, consente la produzione "in house" di materiale video, riproducibile facilmente online. 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.

**Indicazioni operative**

Qualora navigando in Rete si incontri materiale pedopornografico è opportuno segnalarlo, anche anonimamente, attraverso il sito www.generazioniconnesse. it alla sezione Hotline. Questo per facilitare il processo di rimozione del materiale stesso dalla Rete e allo stesso tempo consentire le opportune attività investigative finalizzate ad identificare chi

possiede quel materiale, chi lo diffonde e chi lo produce, ma, soprattutto, ad identificare i minori abusati presenti nelle immagini e video, assicurando la fine di un abuso che potrebbe essere ancora in corso e il supporto necessario. Parallelamente, se si ravvisa un rischio per il benessere psicofisico delle persone minorenni coinvolte nella visione di questi contenuti, sarà opportuno rivolgersi ad un servizio deputato ad offrire un supporto psicologico anche passando per una consultazione presso il medico di base o pediatra di riferimento. Le strutture pubbliche a cui rivolgersi sono i servizi socio-sanitari del territorio di appartenenza (Consultori Familiari, Servizi di Neuropsichiatria infantile, centri specializzati sull'abuso e il maltrattamento all'infanzia, etc.). Nel caso in cui una persona minorenne sia direttamente coinvolta nelle immagini, bisogna tenere in considerazione che l'attuale normativa (legge 172 del 2012, art. 351 c.p.p.) prevede che la persona coinvolta in qualità di vittima o testimone in alcune tipologie di reati, tra cui la pedopornografia online, debba essere ascoltata in sede di raccolta di sommarie informazioni con l'ausilio di una persona esperta in psicologia o psichiatria infantile.

**Il nostro piano d'azioni**

AZIONI (da sviluppare nell'arco dell'anno scolastico 2020/2021).

□ Pianificare e realizzare progetti di peer-education - sui temi della sicurezza online - nella scuola.

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

□ Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse.
□ Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/lle studenti/studentesse.
□ Pianificare e realizzare progetti di peer-education - sui temi della sicurezza online - nella scuola, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti.

## 5. SEGNALAZIONE E GESTIONE DEI CASI

### 5.1. Cosa segnalare

Il personale docente del nostro Istituto quando ha il sospetto o la certezza che uno/a studente/essa possa essere vittima o responsabile di una situazione di cyberbullismo, sexting o adescamento online ha a disposizione procedure definite e può fare riferimento a tutta la comunità scolastica. Questa sezione dell'ePolicy contiene le procedure standardizzate per la segnalazione e gestione dei problemi connessi a comportamenti online a rischio di studenti e studentesse (vedi allegati a seguire). Tali procedure dovranno essere una guida costante per il personale della scuola nell'identificazione di una situazione online a rischio, così da definire le modalità di presa in carico da parte della

scuola e l'intervento migliore da mettere in atto per aiutare studenti/esse in difficoltà. Esse, inoltre, forniscono valide indicazioni anche per i professionisti e le organizzazioni esterne che operano con la scuola (vedi paragrafo 1.3. dell'ePolicy).
Nelle procedure:

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

Inoltre, la scuola individua le figure che costituiranno un team preposto alla gestione della segnalazione (gestione interna alla scuola, invio ai soggetti competenti). Nell'affrontare i casi prevediamo la collaborazione con altre figure, enti, istituzioni e servizi presenti sul territorio (che verranno richiamati più avanti), qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola. Tali procedure sono comunicate e condivise con l'intera comunità scolastica. Questo risulta importante sia per facilitare l'emersione di situazioni a rischio, e la conseguente presa in carico e gestione, sia per dare un messaggio chiaro a studenti e studentesse, alle famiglie e a tutti coloro che vivono la scuola che la stessa è un luogo sicuro, attento al benessere di chi lo vive, in cui le problematiche non vengono ignorate ma gestite con una mobilitazione attenta di tutta la comunità. La condivisione avverrà attraverso assemblee scolastiche che coinvolgono i genitori, gli studenti e le studentesse e il personale della scuola, con l'utilizzo di locandine da affiggere a scuola, attraverso news nel sito della scuola e durante i collegi docenti e attraverso tutti i canali maggiormente utili ad un'efficace comunicazione. A seguire, le problematiche a cui fanno riferimento le procedure allegate:

Cyberbullismo: è necessario capire se si tratta effettivamente di cyberbullismo o di altra problematica. Oltre al contesto, vanno considerate le modalità attraverso le quali il comportamento si manifesta (alla presenza di un "pubblico"? Tra coetanei? In modo ripetuto e intenzionale? C'è un danno percepito alla vittima? etc.). È necessario poi valutare l'eventuale stato di disagio vissuto dagli/lle studenti/esse coinvolti/e (e quindi valutare se rivolgersi ad un servizio deputato ad offrire un supporto psicologico e/o di mediazione).

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

Sexting: nel caso in cui immagini e/o video, anche prodotte autonomamente da persone minorenni, sfuggano al loro controllo e vengano diffuse senza il loro consenso è opportuno adottare sistemi di segnalazione con l'obiettivo primario di tutelare il minore e ottenere la rimozione del materiale, per quanto possibile, se online e il blocco della sua diffusione via dispositivi mobili.

Per quanto riguarda la necessità di segnalazione e rimozione di contenuti online lesivi, ciascun minore ultraquattordicenne (o i suoi genitori o chi esercita la responsabilità del minore) che sia stato vittima di cyberbullismo può inoltrare al titolare del trattamento o al gestore del sito internet o del social media un'istanza per l'oscuramento, la rimozione o il blocco dei contenuti diffusi nella Rete. Se entro 24 ore il gestore non avrà provveduto, l'interessato può rivolgere analoga richiesta al Garante per la protezione dei dati personali, che rimuoverà i contenuti entro 48 ore. I minori potrebbero riferire all'insegnante fatti o eventi personali o altrui, accaduti anche al di fuori della scuola, che potrebbero mettere in allarme il docente. Pertanto, sono da considerare degni di segnalazione:

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

### 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. 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;
- docente referente per le segnalazioni.

Anche studenti e studentesse, inoltre, possono rivolgersi alla Helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96. Per quanto riguarda la gestione dei casi, il nostro Istituto ha individuato una figura referente per il cyberbullismo. La segnalazione del caso dovrà quindi essere fatta dal singolo docente, tramite modulo allegato al presente documento (Allegato 2), alla referente, la quale, insieme al Team per le emergenze, si occuperà di raccogliere tutte le informazioni possibili, anche attraverso colloqui di approfondimento con gli attori coinvolti e di segnalare l'accaduto al Dirigente. Sarà poi il Dirigente, insieme al Team, a valutare se la segnalazione debba essere rivolta ad organi esterni alla scuola quali la Polizia Postale o i Servizi Sociali o se il caso vada gestito all'interno della scuola con il coinvolgimento del Consiglio di Classe e delle famiglie degli alunni coinvolti. Si sceglierà uno o più interventi da attuare a cui seguirà una fase di monitoraggio. (cfr. schema di procedura di intervento nell'Allegato 3)

**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.

**GARANTE REGIONALE PER L'INFANZIA E L'ADOLESCENZA**
**Competenze/Servizi |** Segnala all'autorità giudiziaria i servizi sociali e competenti; accoglie le segnalazioni di presunti abusi; fornisce informazioni sulle modalità di tutela e di esercizio di questi diritti; segnala alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.

**Tipologie di comportamenti al quale risponde l'istituzione/ente/ servizio |** tipologie di comportamenti a rischio: tutte
**Tipologie di comportamenti al quale risponde l'istituzione/ente/ servizio |** tipologie di comportamenti che configurano un reato: tutte

**CORECOM**
**Competenze/Servizi |** Svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale. Tra le varie attività, particolare attenzione è riservata alla tutela dei minori.
**Tipologie di comportamenti al quale risponde l'istituzione/ente/ servizio |** tipologie di comportamenti a rischio: tutte
**Tipologie di comportamenti al quale risponde l'istituzione/ente/ servizio |** tipologie di comportamenti che configurano un reato: cyberbullismo

**UFFICIO SCOLASTICO REGIONALE**
**Competenze/Servizi |** Tra le varie funzioni, supporta la scuola in attività di prevenzione. Può affiancare le scuole nei casi di segnalazione di comportamenti a rischio correlati all'uso di internet.
**Tipologie di comportamenti al quale risponde l'istituzione/ente/ servizio |** tipologie di comportamenti a rischio: cyberbullismo
**Tipologie di comportamenti al quale risponde l'istituzione/ente/ servizio |** tipologie di comportamenti che configurano un reato: cyberbullismo

**TRIBUNALE PER I MINORENNI DI CATANZARO**
**Competenze/Servizi |** Tra le varie attività si occupa di tutti i procedimenti che riguardano reati, misure rieducative, tutela ed assistenza.
**Tipologie di comportamenti al quale risponde l'istituzione/ente/ servizio |** tipologie di comportamenti a rischio: ---
**Tipologie di comportamenti al quale risponde l'istituzione/ente/ servizio |** tipologie di comportamenti che configurano un reato: tutte

**POLIZIA POSTALE E DELLE COMUNICAZIONI**
**Competenze/Servizi |** Si occupa di accogliere tutte le segnalazioni o denunce relative a comportamenti a rischio nell'utilizzo di internet e che si configurano come reati.
**Tipologie di comportamenti al quale risponde l'istituzione/ente/ servizio |** tipologie di comportamenti a rischio: ---
**Tipologie di comportamenti al quale risponde l'istituzione/ente/ servizio |** tipologie di comportamenti che configurano un reato: furto di identità, cyberbullismo (nel caso di cyberstalking), commercio on-line (nel caso di clonazione di

carta di credito), pedopornografia on-line, grooming (adescamento on-line), gioco d'azzardo on-line, sexting.

**AZIENDE SANITARIE LOCALI**

**Competenze/Servizi |** Per avere un sostegno psicologico, psichiatrico o neuropsichiatrico sulle problematiche psicologiche, anche associate all'uso di internet.

**Tipologie di comportamenti al quale risponde l'istituzione/ente/ servizio |** tipologie di comportamenti a rischio: tutte

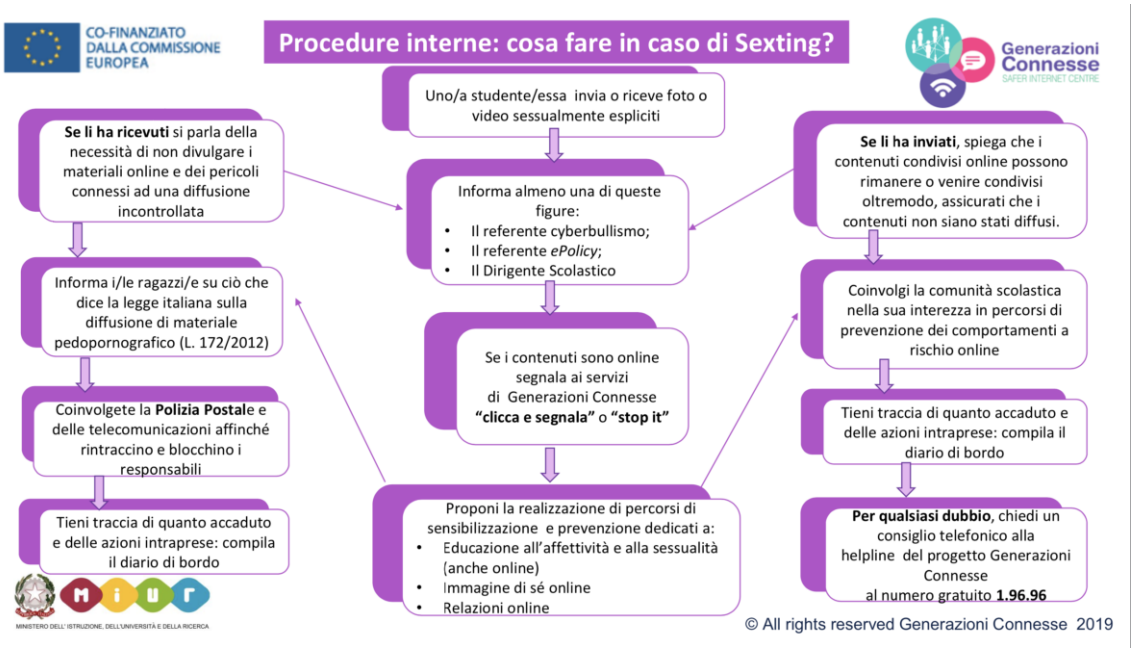
**Tipologie di comportamenti al quale risponde l'istituzione/ente/ servizio |** tipologie di comportamenti che configurano un reato: tutte

Nei casi di maggiore gravità, si valuterà anche il coinvolgimento di attori esterni quali Forze dell'ordine e Servizi sociali. I documenti relativi alle procedure operative e i protocolli sono da elaborare in collaborazione con i suddetti attori del territorio, con cui siglarli unitamente.

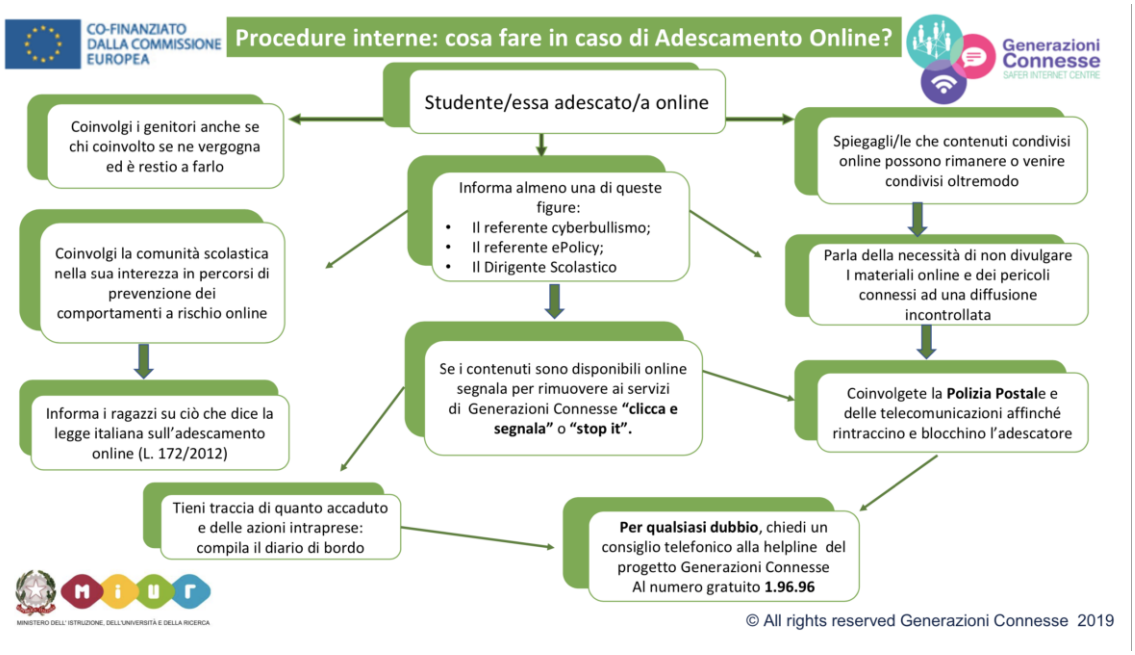
## 5.4. - Allegati con le procedure

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

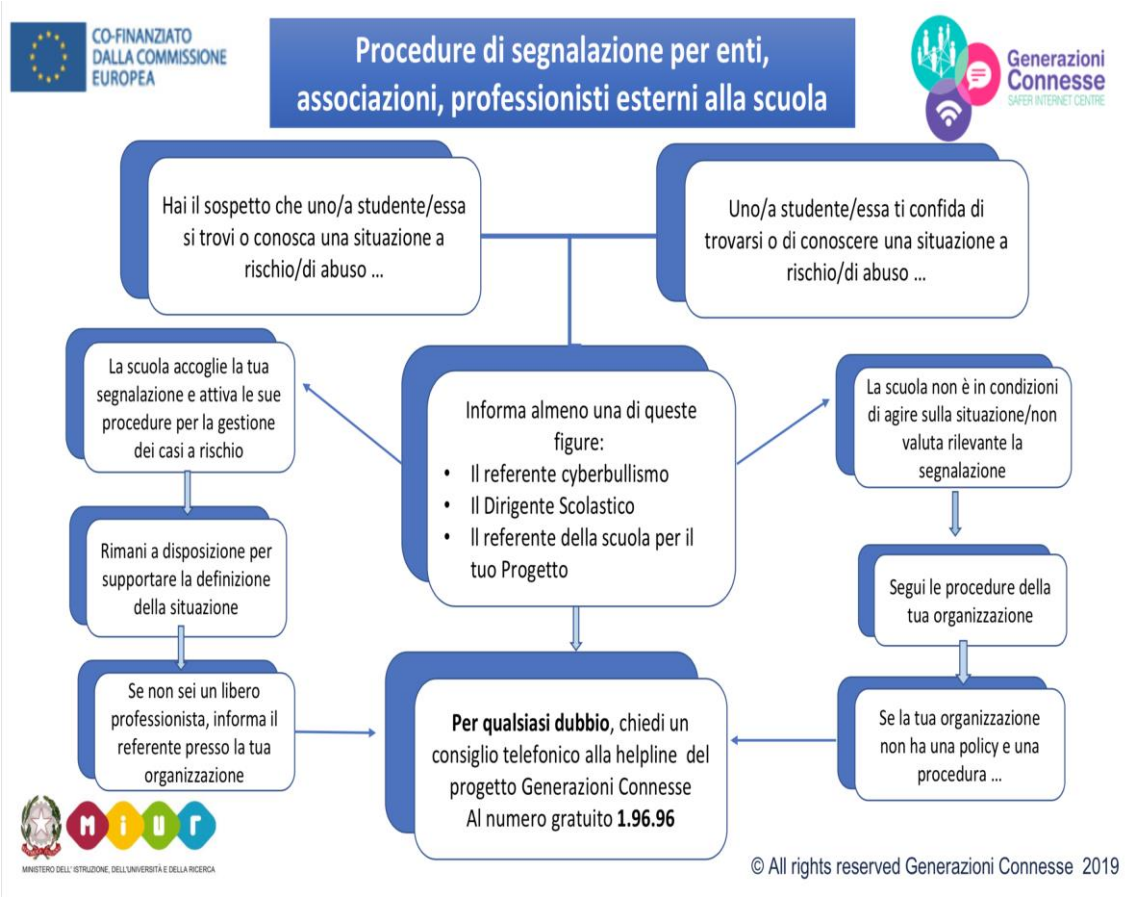
## Procedure interne: cosa fare in caso di sexting?




## Procedure interne: cosa fare in caso di adescamento online



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



Altri allegati

**Prima segnalazione dei casi di (presunto) bullismo e vittimizzazione**

Nome di chi compila la segnalazione:

Data:

Scuola:

1. La persona che ha segnalato il caso di presunto bullismo era
❑ La vittima
❑ Un compagno della vittima, nome_____
❑ Madre/ Padre/Tutore della vittima, nome_____
❑ Insegnante, nome _____
❑ Altri: _____

2. Vittima _____Classe____
Altre vittime _____Classe_____
Altre vittime _____Classe_____

3. Bullo o i bulli (o presunti)
Nome_____Classe____
Nome_____Classe____
Nome_____Classe____

4. Descrizione breve del problema presentato. Dare esempi concreti degli episodi di prepotenza.
_____
_____
_____
_____

5. Quante volte sono successi gli episodi?
_____

**PROCEDURA PER CASO DI PRESUNTO BULLISMO E VITTIMIZZAZIONE A SCUOLA**

1. Prima segnalazione
2. Valutazione approfondita
3. Gestione del caso attraverso uno o più interventi:
    - Approccio educativo con la classe
    - Intervento individuale
    - Gestione della relazione
    - Coinvolgimento la famiglia
    - Supporto intensivo a lungo termine e di rete
4. Monitoraggio