Approvato con delibera n.7 del Consiglio di Istituto del 17 ottobre 2020

Documento di ePolicy

AVIC86200D

Istituto Comprensivo Statale "P.S. MANCINI"

VIA CARDITO - 83031 - ARIANO IRPINO - AVELLINO (AV)

Massimiliano Bosco

Capitolo 1 - Introduzione al documento di ePolicy

Premessa

La tecnologia digitale nel mondo della scuola ha innovato la modalità di apprendere, di ricercare e approcciare alla conoscenza e ha rivoluzionato la didattica offrendo un valido strumento e supporto nello studio grazie all'integrazione dei linguaggi tipici del digitale: immagini, testo, audio, video. Il nostro istituto, percependo l'evoluzione del mondo della

comunicazione, ha sempre posto una forte attenzione all'uso delle nuove tecnologie nella didattica riconoscendo gli evidenti benefici che esse promuovono nei processi di insegnamento/apprendimento. Tutti i nostri studenti hanno accesso alle reti informatiche e possono avvalersi della tecnologia in qualsiasi momento della giornata scolastica e sempre con la guida del personale docente. L'obiettivo della nostra scuola è di assicurare sempre e nel miglior modo un'interazione positiva e adeguata con le TIC e di condurre gli studenti ad un uso corretto e consapevole della tecnologia. L'istituto Mancini è stato sempre attivo e sensibile nello studio, al confronto di tematiche e rischi legati alle nuove tecnologie: ha partecipato al progetto Cyberkid, progetto Moige sul cyberbullismo; la rilevazione interna di dati sull'utilizzo di dispositivi è inoltre, periodica e pianificata; negli ultimi due anni sono stati sostenuti corsi di aggiornamento per i docenti in merito all'utilizzo delle TIC nella didattica e all'utilizzo sicuro e positivo di Internet e delle tecnologie digitali; sono state emanate norme interne riguardo l'uso ed abuso dei dispositivi informatici nel Regolamento d'Istituto e nel Patto di corresponsabilità; ai genitori viene consegnata l'informativa sul trattamento dei dati personali (ai sensi dell'art. 13 del D. Lgs. 30 giugno 2003, n. 196), e richiesta di autorizzazione all'utilizzo dei dati personali degli alunni eccedenti i trattamenti istituzionali obbligatori, come per esempio l'utilizzo di fotografie, video o altri materiali audiovisivi contenenti l'immagine, il nome e/o la voce del proprio figlio/a, all'interno di attività educative e didattiche per scopi documentativi, formativi e informativi, durante gli anni di frequenza della scuola.

1.1 - Scopo dell'ePolicy

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

Le "competenze digitali" sono fra le abilità chiave all'interno del Quadro di riferimento Europeo delle Competenze per l'apprendimento permanente e di esse bisogna dotarsi proprio a partire dalla scuola (Raccomandazione del Consiglio Europeo del 2006 aggiornata al 22 maggio 2018, relativa alle competenze chiave per l'apprendimento permanente). In un contesto sempre più complesso, diventa quindi essenziale per ogni Istituto Scolastico dotarsi di una E-policy, un documento programmatico volto a promuovere le competenze digitali ed un uso delle tecnologie positivo, critico e consapevole, sia da parte dei ragazzi e delle ragazze che degli adulti coinvolti nel processo educativo. L'E-policy, inoltre, vuole essere un documento finalizzato a prevenire situazioni problematiche e a riconoscere, gestire, segnalare e monitorare episodi legati ad un utilizzo scorretto degli strumenti. L'E-policy ha l'obiettivo di esprimere la nostra visione educativa e proposta formativa, in riferimento alle tecnologie digitali.

Nello specifico:

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

Argomenti del Documento

5. Sexting
6. Adescamento online
7. Pedopornografia

5. Segnalazione e gestione dei casi

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

Perché è importante dotarsi di una E-policy?

Attraverso l'E-policy il nostro Istituto si vuole dotare di uno strumento operativo a cui tutta la comunità educante dovrà fare riferimento, al fine di assicurare un approccio alla tecnologia che sia consapevole, critico ed efficace, e al fine di sviluppare, attraverso specifiche azioni, una conoscenza delle opportunità e dei rischi connessi all'uso di Internet. L' E-policy fornisce, quindi, delle linee guida per garantire il benessere in Rete, definendo regole di utilizzo delle TIC a scuola e ponendo le basi per azioni formative e educative su e con le tecnologie digitali, oltre che di sensibilizzazione su un uso consapevole delle stesse.

1.2 - Ruoli e responsabilità

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

IL DIRIGENTE SCOLASTICO

Garantisce la sicurezza di tutti i membri della comunità scolastica, anche online. Promuove la cultura della sicurezza e sulla prevenzione di problematiche offline e online e organizza, insieme al referente del bullismo, corsi di formazione specifici, sulle tematiche del bullismo e cyberbullismo, per tutte le figure scolastiche sull'utilizzo positivo e responsabile delle TIC. Il Dirigente Scolastico gestisce e interviene nei

casi di gravi episodi di bullismo e di cyberbullismo ed uso improprio delle tecnologie digitali.

L'ANIMATORE DIGITALE

Promuove percorsi di formazione interna all'istituto negli ambiti di sviluppo della scuola digitale; monitora e rileva eventuali episodi o problematiche connesse all'uso delle TIC; controlla che gli utenti autorizzati accedono alla Rete a scuola con apposite Password per scopi istituzionali e consentiti. Supporta il personale scolastico nella prevenzione dei rischi online e alla protezione e gestione dei dati personali.

REFERENTE BULLISMO E CYBERBULLISMO

Il Referente bullismo e cyberbullismo coordina le iniziative di prevenzione e contrasto al bullismo e cyberbullismo (art. 4 Legge 71/2017), avvalendosi anche della collaborazione delle Forze di polizia, delle associazioni e dei centri di aggregazione giovanile del territorio. Promuove progetti e percorsi formativi per gli studenti, personale scolastico e genitori sulle tematiche del bullismo e cyberbullismo.

DOCENTI

I docenti hanno il compito di diffondere la cultura dell'uso responsabile delle TIC e della Rete; promuovono l'uso delle tecnologie digitali nella didattica, laddove possibile; accompagnano e supportano gli alunni nelle attività di apprendimento e nei laboratori che prevedono l'uso della LIM o di altri dispositivi tecnologici che si connettono alla rete; segnalano al Dirigente Scolastico eventuali problematiche, violazioni o abuso, anche online, che vede coinvolti gli alunni.

IL PERSONALE TECNICO AMMINISTRATIVO E AUSILIARE

Il personale ATA è concretamente coinvolto nel tempo scuola, nell'offerta formativa e, come dispone la legge 107/2015 (la Buona

scuola) anche nella formazione e autoformazione in tema di bullismo e di cyberbullismo., All'interno del regolamento d'Istituto, il personale ATA è coinvolto nella segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo, e nel raccogliere, verificare e valutare le informazioni inerenti a possibili casi di bullismo/cyberbullismo.

GLI ALUNNI
Gli alunni, in relazione al proprio grado di maturità e consapevolezza raggiunta, utilizzano al meglio le tecnologie digitali in coerenza con quanto richiesto dai docenti; con il supporto della scuola imparano a tutelarsi online, tutelare i/le propri/e compagni/e e rispettarli/le; partecipano attivamente a progetti ed attività che riguardano l'uso positivo delle TIC e della Rete e sono promotori di quanto appreso attraverso percorsi di peer education;

I GENITORI
In continuità con l'Istituto scolastico, i genitori sono partecipi e attivi nelle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete; si relazionano in modo costruttivo con i docenti sulle linee educative che riguardano le TIC e la Rete e comunicano con loro circa i problemi rilevati quando i/le propri/e figli/e non usano responsabilmente le tecnologie digitali o Internet. Accettano e condividono quanto scritto nell'ePolicy dell'Istituto.

GLI ENTI EDUCATIVI ESTERNI E LE ASSOCIAZIONI
Tutti gli enti educativi esterni e le varie associazioni presenti sul territorio che entrano in relazione con il nostro Istituto si conformano alla politica riguardo all'uso delle TIC e della Rete che la scuola ha condiviso; promuovono comportamenti sicuri, la sicurezza online e assicurano la protezione degli alunni durante le attività che si svolgono insieme.

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

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

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

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

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

1.4 - CONDIVISIONE E COMUNICAZIONE DELL'EPOLICY ALL'INTERA COMUNITÀ SCOLASTICA

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

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

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

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

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

1.5 - Gestione delle infrazioni alla ePolicy

La scuola gestirà le infrazioni all'E-policy attraverso azioni educative e/o sanzioni, qualora fossero necessarie, valutando i diversi gradi di gravità di eventuali violazioni. Sarà valutata la necessità di denunciare l'episodio e/o di garantire immediato supporto psicologico all' alunno attraverso i servizi predisposti, qualora ciò fosse necessario. Saranno valutati anche le possibili infrazioni nelle quali il personale scolastico e soprattutto i docenti possono incorrere utilizzando la rete, nonché in quelle violazioni qualora non intervengano nella segnalazione di condotte improprie degli alunni.

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. Si allegano all'epolicy i vari regolamenti scolastici aggiornati alla luce del regolamento redatto.

1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

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

Il nostro piano d'azioni

Il nostro Istituto organizzerà:

- attività volte a presentare il progetto di Generazioni Connesse e consultare i docenti dell'istituto per la stesura finale del documento e-policy.
- un evento di presentazione del progetto di Generazioni Connesse agli studenti, ai genitori, a tutta la comunità scolastica e alle varie agenzie educative presenti sul territorio allo scopo di sensibilizzare e ampliare la conoscenza verso temi importanti come la privacy, il bullismo, il cyberbullismo.

Capitolo 2 - Formazione e curricolo

2.1. Curricolo sulle competenze digitali per gli studenti

I ragazzi usano la Rete quotidianamente, talvolta in modo più "intuitivo" ed "agile" rispetto agli adulti, ma non per questo sono dotati di maggiori "competenze digitali". Infatti, "la competenza digitale presuppone l'interesse per le tecnologie digitali e il loro utilizzo con dimestichezza e spirito critico e responsabile per apprendere, lavorare e partecipare alla società. Essa comprende l'alfabetizzazione informatica e digitale, la comunicazione e la collaborazione, l'alfabetizzazione mediatica, la creazione di contenuti digitali (inclusa la programmazione), la sicurezza (compreso l'essere a proprio agio nel mondo digitale e possedere competenze relative alla cybersicurezza), le questioni legate alla proprietà intellettuale, la risoluzione di problemi e il pensiero critico" ("Raccomandazione del Consiglio europeo relativa alla competenze chiave per l'apprendimento permanente", C189/9, p.9). Per questo la scuola si impegna a portare avanti percorsi volti a promuovere tali competenze, al fine di educare gli studenti e le studentesse verso un uso consapevole e responsabile delle tecnologie digitali. Ciò avverrà attraverso la progettazione e implementazione di un curricolo digitale. Esso sarà continuativo e trasversale alle varie discipline. Sarà implementato sulle cinque aree del quadro di riferimento europeo DigComp versione 2.1:

1)alfabetizzazione su informazioni e dati;
2)comunicazione e collaborazione;
3)creazione di contenuti digitali;
4)sicurezza;
5)risolvere problemi.

Di queste aree sarà data maggiore rilevanza alla consapevolezza dei rischi e delle possibili minacce che si innescano nel momento in cui ci connettiamo a internet: ciò che ignorano i nativi digitali è principalmente la competenza sulla sicurezza online e sui rischi che ciò comporta. La rete è il luogo della socialità, è parte integrante del loro contesto esperenziale

e contribuisce in modo rilevante alla costruzione della propria identità, ma è anche il luogo dove si rischia di essere vittime di cyberbullismo. Il tema della sicurezza online sarà affrontato con tutti gli alunni dell'istituto, a partire dalla classe terza della scuola primaria perché sarà nostro obiettivo creare a scuola una cultura della sicurezza in rete. La competenza sulla protezione dei dati personali e della privacy sarà un'ancella nella revisione del nostro Curricolo digitale.

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

È fondamentale che i docenti tutti siano formati ed aggiornati sull'uso corretto, efficace ed efficiente delle TIC nella didattica, al fine di usarle in modo integrativo ed inclusivo. Ciò si rende necessario per fornire agli studenti e alle studentesse modelli di utilizzo positivo, critico e specifico delle nuove tecnologie e per armonizzare gli apprendimenti. Ciò comporta che tutti gli insegnanti raggiungano un buon livello di formazione sull'uso corretto, efficace ed efficiente delle TIC nella didattica. Atteso ciò, il nostro istituto riconosce e favorisce la partecipazione della comunità educante ad iniziative promosse sia direttamente dalla scuola, dalle reti di scuole, sia quelle liberamente scelte dai docenti (anche online), sempre coerenti con il piano di formazione.

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. Dotare i docenti di strumenti per poter educare gli alunni alle emozioni in contesto online è importante: oggi i ragazzi comunicano, si esprimono e sviluppano la loro identità personale e sociale attraverso le nuove tecnologie che sempre più permettono loro di entrare in contatto con il mondo che lo circonda.

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

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

Il nostro piano d'azioni

Azioni che l'istituto svilupperà nell'arco di un anno (2019/2020).

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

2) Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica

Azioni che l'istituto svolgerà nell'arco di un triennio:

1) Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.

2) Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali. Numero di docenti da raggiungere = 70%

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

3.1 - Protezione dei dati personali

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

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

Ogni giorno a scuola vengono trattati numerosi dati personali sugli studenti e sulle loro famiglie. Talvolta, tali dati possono riguardare informazioni sensibili, come problemi sanitari o particolari disagi sociali. Il "corretto trattamento dei dati personali" a scuola è condizione necessaria per il rispetto della dignità delle persone, della loro identità e del loro diritto alla riservatezza. Per questo è importante che le istituzioni

scolastiche, durante lo svolgimento dei loro compiti, rispettino la privacy, tutelando i dati personali dei soggetti coinvolti, in particolar modo quando questi sono minorenni. La protezione dei dati personali è un diritto fondamentale dell'individuo ai sensi della Carta dei diritti fondamentali dell'Unione europea (art. 8), tutelato dal Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 (relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati). Anche le scuole, quindi, hanno oggi l'obbligo di adeguarsi al cosiddetto GDPR (General Data Protection Regulation) e al D.Lgs. 10 agosto 2018, n. 101, entrato in vigore lo scorso 19 settembre. In questo paragrafo dell'ePolicy affrontiamo tale problematica, con particolare riferimento all'uso delle tecnologie digitali, e indichiamo le misure che la scuola intende attuare per garantire la tutela della privacy e il diritto alla riservatezza di tutti i soggetti coinvolti nel processo educativo, con particolare attenzione ai minori. A tal fine, l'Istituto allega alla presente ePolicy i modelli di liberatoria da utilizzare e conformi alla normativa vigente, in materia di protezione dei dati personali. La velocità, l'immediatezza con cui si risponde ai messaggi o si condividono foto o video, può far perdere il controllo di dati personali e mettere a rischio la reputazione e la sicurezza dei soggetti coinvolti. Tenendo fede al Regolamento UE 2016/679, l'istituto redige e mantiene un registro dei trattamenti dei dati: sia per il titolare che per il responsabile; valuta i rischi sulla privacy; analizza il sito web istituzionale di riferimento con proposte volte a migliorare la sicurezza e la protezione dei dati trattati. Le nostre proposte di messa insicurezza della intranet scolastica sono:

-la white list per la navigazione come sistema di filtraggio dei contenuti;
-la firewall hardware che è una componente hardware che, utilizzando un certo insieme di regole predefinite, permette di filtrare ed eventualmente bloccare tutto il traffico da e verso una qualsiasi rete di computer lasciando passare solo tutto ciò che rispetta determinate regole; - corsi di formazione destinati ai responsabili, agli incaricati del trattamento dei dati personali

3.2 - Accesso ad Internet

1. L'accesso a Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale.
2. Ogni persona ha eguale diritto di accedere a Internet in condizioni di parità, con modalità tecnologicamente adeguate e aggiornate che rimuovano ogni ostacolo di ordine economico e sociale.
3. Il diritto fondamentale di accesso a Internet deve essere assicurato nei suoi presupposti sostanziali e non solo come possibilità di collegamento alla Rete.
4. L'accesso comprende la libertà di scelta per quanto riguarda dispositivi, sistemi operativi e applicazioni anche distribuite.
5. Le Istituzioni pubbliche garantiscono i necessari interventi per il superamento di ogni forma di divario digitale tra cui quelli determinati dal genere, dalle condizioni economiche oltre che da situazioni di vulnerabilità personale e disabilità. Così recita l'art. 2 della Dichiarazione dei diritti di Internet, elaborata dalla Commissione per i diritti e i doveri in Internet, commissione costituita il 27 ottobre 2014 presso la Camera dei Deputati dalla presidente Laura Boldrini e presieduta da Stefano Rodotà. Inoltre, il 30 aprile 2016 era entrato in vigore il Regolamento UE del Parlamento Europeo e del Consiglio del 25 novembre 2015, che stabilisce le "misure riguardanti l'accesso a un'Internet aperto e che modifica la direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica e il regolamento (UE) n. 531/2012 relativo al roaming sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione". Il diritto di accesso a Internet è dunque presente nell'ordinamento italiano ed europeo e la scuola dovrebbe essere il luogo dove tale diritto è garantito, anche per quegli studenti che non dispongono della Rete a casa. In modo coerente il PNSD (Piano Nazionale Scuola Digitale) ha tra gli obiettivi quello di "fornire a tutte le scuole le condizioni per l'accesso alla società dell'informazione e fare in modo che il "diritto a Internet" diventi una realtà, a partire dalla scuola". Questo perché le tecnologie da un lato contribuiscono a creare un ambiente che può rendere la scuola aperta, flessibile e inclusiva, dall'altro le consentono di adeguarsi ai cambiamenti della società e del mercato del lavoro,

puntando a sviluppare una cultura digitale diffusa che deve iniziare proprio a scuola. L'istituto garantisce il diritto di ogni studente di connettersi a Internet in quanto in tutte le classi sono presenti Lim collegate a rete Wi-fi con connessione a banda larga; predispone di laboratori informatici e linguistici che rispondono alle reali esigenze didattiche e agli obiettivi prefissati. Ogni aggiornamento dell'infrastruttura tecnologica avviene con una pianificazione a lungo termine e con il necessario coinvolgimento dell'animatore digitale e del tecnico informatico. In riferimento alla security la scuola presta attenzione a tutti gli aspetti che riguardano la gestione degli account degli utenti. A tale documento è allegato un regolamento d'istituto sull'uso delle TIC. Gli interventi periodici di manutenzione vengono pianificati e i problemi tecnici quotidiani legati all'uso della strumentazione vengono affrontati attraverso una formazione, non solo sull'uso della tecnologia nella didattica ma anche nell'uso della tecnologia in sé. Per tutti gli alunni minori di 16 anni la scuola richiede il consenso scritto genitoriale all'uso di internet. Ogni accesso a internet va adeguato all'età degli studenti e la scuola prende le necessarie precauzioni per evitare l'accesso online a materiali non adatti a loro all'interno della scuola attraverso sistemi di filtraggio.

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. Sussistono due tipi di comunicazione online: una esterna ed una interna alla scuola. Quella esterna si concretizza in primis attraverso il sito web dell'istituto, una web-radio, una pagina facebook. Essa è progettata per comunicare e trasmettere all'esterno l'identità, i valori e le azioni, i progetti e l'idea di educazione che la l'istituto porta avanti. La

comunicazione interna avviene attraverso il registro elettronico, le e-mail, piattaforme di lavoro condiviso e collaborativo, attraverso gruppi whatsApp tra docenti. Il registro elettronico gestisce buona parte della comunicazione con le famiglie, attraverso cui possono visualizzare molte informazioni utili, interagendo con la scuola. In entrambe le modalità di comunicazione vanno rispettate le seguenti regole elaborate e condivise da tutta la comunità scolastica.

-Nella comunicazione di gruppo bisogna rispettare sempre le finalità del gruppo, scrivendo e pubblicando solo contenuti pertinenti a tali finalità:

-Usare sempre un linguaggio adeguato e il più possibile chiaro e preciso

-Utilizzare il gruppo come una bacheca virtuale, pubblicando solo avvisi, informazioni e iniziative che riguardano la sezione/classe

-Non condividere file multimediali troppo pesanti;

-Evitare il più possibile di condividere foto di studenti in chat;

-Indirizzare solo domande precise e chiare, a cui si possano dare risposte altrettanto brevi e precise;

-Utilizzare messaggi brevi ed esaustivi allo stesso tempo.

Per le chat formali, create dal Dirigente scolastico per veicolare informazioni e aggiornamenti riferiti all'attività scolastica, la regolamentazione è prevista dalla contrattazione d'istituto.

Il registro elettronico va utilizzato per comunicare alle famiglie:

-l'andamento scolastico (assenze, argomenti lezioni e compiti, note disciplinari);

-risultati scolastici (voti, documenti di valutazione);

-le udienze (prenotazioni colloqui individuali);

-gli eventi (agenda eventi);

-comunicazione varie (comunicazioni di classe, comunicazioni personali)

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.

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 a tenere il dispositivo (smartphone) spento quando sono a scuola, indipendentemente dall'attività svolta (lezione, ricreazione, accesso ai servizi igienici, pause, ecc.).

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". Il Patto educativo di corresponsabilità introdotto con DPR 235 del 2007, va letto anche in riferimento all'educazione dei ragazzi e delle ragazze all'uso dei nuovi dispositivi tecnologici, inclusi tablet e smartphone sia a scuola che a casa. Pertanto si rende noto che La diffusione di filmati e foto che ledono la riservatezza e la dignità delle persone può far incorrere lo studente in sanzioni disciplinari e pecuniarie o perfino in veri e propri reati. Stesse cautele vanno previste per l'uso dei tablet, se usati a fini di registrazione e non soltanto per fini didattici o per consultare in classe libri elettronici e testi on line". Resta la responsabilità deontologica e professionale del dirigente, dei docenti e del personale ATA che hanno il dovere di vigilare sui comportamenti degli studenti e delle studentesse il quale sussiste in tutti gli spazi scolastici e di segnalare eventuali infrazioni suscettibili di sanzioni disciplinari. La nostra scuola, in collaborazione con le famiglie e con gli enti locali si apre al cosiddetto BYOD ossia a politiche per cui

l'utilizzo di dispositivi elettronici personali durante le attività didattiche sia possibile ed efficace. I docenti non possono utilizzare il dispositivo smartphone a scuola durante le ore di lezione come disposto dalla Circolare n° 362 del 25 agosto 1998. E' consentito l'uso di altri dispositivi personali elettronici solo per uso didattico. Per il restante orario di servizio è consentito l'uso del dispositivo (smartphone) solo per importanti comunicazioni personali urgenti.

Il nostro piano d'azioni

Azioni da svolgere nell'anno scolastico 2019/2020

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli alunni
- Organizzare incontri per la consultazione dei genitori su indicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola

Azioni da svolgere nel triennio 2019-20 2020-21 2021-22

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

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

4.1 - Sensibilizzazione e Prevenzione

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

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

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

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

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

<u>Interventi di sensibilizzazione da mettere in campo:</u>

coinvolgere un gruppo ristretto di persone per mettere in luce la problematica del cyberbullismo e della violazione della privacy affinché agiscano insieme in favore di una causa in cui credono.

<u>Interventi di prevenzione:</u>

La prevenzione va posta in modo universale, cioè mirata e programmata con interventi ad un grande gruppo di studenti; in modo selettivo, cioè

mirata ad un piccolo gruppo di studenti in cui il rischio online è presente; in modo indicato, cioè riferibile ad uno specifico caso con l'obiettivo di ridurre i comportamenti problematici.

4.2 - Cyberbullismo: che cos'è e come prevenirlo

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

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

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

- formazione del personale scolastico, prevedendo la partecipazione di un proprio referente per ogni autonomia scolastica;
- sviluppo delle competenze digitali, tra gli obiettivi formativi prioritari (L.107/2015);
- promozione di un ruolo attivo degli studenti (ed ex studenti) in attività di peer education;
- previsione di misure di sostegno e rieducazione dei minori coinvolti;
- Integrazione dei regolamenti e del patto di corresponsabilità con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti;

Il sistema scolastico deve prevedere azioni preventive ed educative e non solo sanzionatorie e 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. A tal fine, può avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio.

Il referente di bullismo e cyberbullismo potrà svolgere un importante compito di supporto al dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d'istituto), atti e documenti (PTOF, PdM, Rav).

Salvo che il fatto costituisca reato, il Dirigente Scolastico qualora venga a conoscenza di atti di cyberbullismo deve informare tempestivamente i genitori dei minori coinvolti (art.5).

Ogni eventuale stato di disagio vissuto da un minore sarà valutato dai servizi socio-sanitari presenti sul territorio, organi deputati a offrire un supporto psicologico e/o di mediazione. Inoltre, 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 il gestore non avrà provveduto, l'interessato può rivolgere analoga richiesta al Garante per la protezione dei dati personali, che rimuoverà i contenuti entro 48 ore. Si allega modello per la segnalazione/reclamo in materia si cyberbullismo da inviare a: cyberbullismo@gpdp.it.

Nel caso in cui si ipotizzi che ci si possa trovare di fronte ad una fattispecie di reato (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. È in tal senso possibile far riferimento a queste tipologie di uffici: Polizia di Stato – Compartimento di Polizia postale e delle Comunicazioni; 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).

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

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

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

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

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere in relazione a questa problematica. Il processo formativo degli alunni sarà implementato con percorsi educativi finalizzati a valorizzare la parità di genere, la diversità vissuta come originalità e identità di ogni persona. Sarà promossa una politica di inclusione estesa a non solo a tutta la comunità scolastica ma coinvolgerà la famiglia e il territorio.

4.4 - Dipendenza da Internet e gioco online

La Dipendenza da Internet fa riferimento all'utilizzo eccessivo e incontrollato di Internet che, al pari di altri comportamenti patologici/dipendenze, può causare o essere associato a isolamento sociale, sintomi da astinenza, problematiche a livello scolastico e irrefrenabile voglia di utilizzo della Rete. L'istituto è intenzionato a promuovere azioni di prevenzione attraverso percorsi sul benessere digitale. Se da un lato La tecnologia ha modificato gli ambienti che viviamo e ha un impatto sulla qualità della vita, parallelamente la scuola intende valorizzare gli elementi che contribuiscono al benessere digitale che sono:

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

Questo è un argomento trasversale che sarà affrontato quando si parlerà di cittadinanza digitale, di cyberbullismo, di uso integrativo e non sostitutivo dei dispositivi e della Rete; dedicheremo al tema un momento specifico e riflettere con studenti e studentesse per fare in modo che la tecnologia sia strumento per raggiungere i propri obiettivi e non sia solo distrazione o addirittura ostacolo.
La scuola da questo punto di vista integra la tecnologia nella didattica, mostrando un suo utilizzo funzionale che possa rendere più consapevoli i ragazzi e le ragazze delle proprie abitudini online.

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. La consapevolezza che delle proprie immagini personali possano essere condivise e permanere online danneggia in termini psicologici e sociali sia il soggetto della foto che colui che ha diffuso i materiali online. La Legge 19 luglio 2019 n. 69, all'articolo 10 ha introdotto in Italia il reato di revenge porn, con la denominazione di diffusione illecita di immagini o di video sessualmente espliciti. Per proteggere i ragazzi dai rischi della rete è di fondamentale importanza implementare a scuola delle azioni di prevenzione, coinvolgendo genitori, insegnanti e professionisti dell'infanzia con lo scopo di creare una rete di sensibilizzazione al problema e di educazione al buon uso della rete.

4.6 - Adescamento online

Il grooming (dall'inglese "groom" - curare, prendersi cura) rappresenta una tecnica di manipolazione psicologica che gli adulti potenziali abusanti utilizzano per indurre i bambini/e o adolescenti a superare le resistenze emotive e instaurare una relazione intima e/o sessualizzata. Gli adulti interessati sessualmente a bambini/e e adolescenti utilizzano spesso anche gli strumenti messi a disposizione dalla Rete per entrare in contatto con loro. I luoghi virtuali in cui si sviluppano più frequentemente tali dinamiche sono le chat, anche quelle interne ai giochi online, i social network in generale, le varie app di instant messaging (whatsapp, telegram etc.), i siti e le app di teen dating (siti di incontri per adolescenti). Un'eventuale relazione sessuale può avvenire, invece, attraverso webcam o live streaming e portare anche ad incontri dal vivo. In questi casi si parla di adescamento o grooming online. In Italia l'adescamento si configura come reato dal 2012 (art. 609-undecies – l'adescamento di minorenni) quando è stata ratificata la Convenzione di Lanzarote (legge 172 del 1° ottobre 2012).

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere per prevenire ed affrontare la delicata problematica dell'adescamento. -Affrontare il tema dell'adescamento online attraverso incontri con esperti a scuola. -Condurre i ragazzi verso una maggiore consapevolezza dei rischi della comunicazione sul web, programmando anche interventi educativi sulla concretizzazione del processo di adescamento online. Redigere con gli alunni una netiquette sui comportamenti da osservare online

4.7 - Pedopornografia

La pedopornografia online è un reato (art. 600-ter comma 3 del c.p.) che consiste nel produrre, divulgare, diffondere e pubblicizzare, anche per via telematica, immagini o video ritraenti bambini/e, ragazzi/e coinvolti/e in comportamenti sessualmente espliciti, concrete o simulate o qualsiasi rappresentazione degli organi sessuali a fini soprattutto sessuali. La legge n. 269 del 3 agosto 1998 "Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di schiavitù", introduce nuove fattispecie di reato (come ad esempio il turismo sessuale) e, insieme alle successive modifiche e integrazioni contenute nella legge n. 38 del 6 febbraio 2006 "Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet", segna una tappa fondamentale nella definizione e predisposizione di strumenti utili a contrastare i fenomeni di sfruttamento sessuale a danno di minori. Quest'ultima, introduce, tra le altre cose, il reato di "pornografia minorile virtuale" (artt. 600 ter e 600 quater c.p.) che si verifica quando il materiale pedopornografico rappresenta immagini relative a bambini/e ed adolescenti, realizzate con tecniche di elaborazione grafica non associate, in tutto o in parte, a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali. Secondo la Legge 172/2012 - Ratifica della Convenzione di Lanzarote (Art 4.) per pornografia minorile si intende ogni rappresentazione, con qualunque mezzo, di un minore degli

anni diciotto coinvolto in attività sessuali esplicite, reali o simulate, o qualunque rappresentazione degli organi sessuali di un minore di anni diciotto per scopi sessuali.

In un'ottica di attività preventive, il tema della pedopornografia è estremamente delicato, occorre parlarne sempre in considerazione della maturità, della fascia d'età e selezionando il tipo di informazioni che si possono condividere. La pedopornografia è tuttavia un fenomeno di cui si deve sapere di più, ed è utile parlarne, in particolare se si vogliono chiarire alcuni aspetti legati alle conseguenze impreviste del sexting. Inoltre, è auspicabile che possa rientrare nei temi di un'attività di sensibilizzazione rivolta ai genitori e al personale scolastico promuovendo i servizi di Generazioni Connesse: qualora navigando in Rete si incontri materiale pedopornografico è opportuno segnalarlo, anche anonimamente, attraverso il sito www.generazioniconnesse.it alla sezione "Segnala contenuti illegali" (Hotline).

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

Il nostro piano d'azioni

-Programmare interventi di sensibilizzazione al problema coinvolgendo le famiglie

-Utilizzare sistemi di filtraggio alla rete web della scuola

-Promuovere i servizi di Generazioni Connesse al personale scolastico e alle famiglie per segnalare eventuali materiali pedopornografici incontrati in rete

Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

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

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

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

Nelle procedure sono indicate:

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

Inoltre, la scuola individua le figure che costituiranno un team preposto alla gestione della segnalazione (gestione interna alla scuola, invio ai soggetti competenti). Nell'affrontare i casi prevediamo la collaborazione con altre figure, enti, istituzioni e servizi presenti sul territorio (che verranno richiamati più avanti), qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.

Tali procedure sono comunicate e condivise con l'intera comunità scolastica. Questo risulta importante sia per facilitare l'emersione di situazioni a rischio, e la conseguente presa in carico e gestione, sia per dare un messaggio chiaro a studenti e studentesse, alle famiglie e a tutti coloro che vivono la scuola che la stessa è un luogo sicuro, attento al benessere di chi lo vive, in cui le problematiche non vengono ignorate ma gestite con una mobilitazione attenta di tutta la comunità. La condivisione avverrà attraverso assemblee scolastiche che coinvolgono i genitori, gli studenti e le studentesse e il personale della scuola, con l'utilizzo di locandine da affiggere a scuola, attraverso news nel sito della scuola e durante i collegi docenti e attraverso tutti i canali maggiormente utili ad un'efficace comunicazione.

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

- Cyberbullismo: è necessario capire se si tratta effettivamente di cyberbullismo o di altra problematica. Oltre al contesto, vanno considerate le modalità attraverso le quali il comportamento si manifesta (alla presenza di un "pubblico"? Tra coetanei? In modo ripetuto e intenzionale? C'è un danno percepito alla vittima? etc.). È necessario poi valutare l'eventuale stato di disagio vissuto dagli/lle studenti/esse coinvolti/e (e quindi valutare se rivolgersi ad un servizio deputato ad offrire un supporto psicologico e/o di mediazione).
- Adescamento online: se si sospetta un caso di adescamento online è opportuno, innanzitutto, fare attenzione a non cancellare eventuali prove da smartphone, tablet e computer utilizzati dalla persona minorenne e inoltre è importante non sostituirsi al bambino/a e/o adolescente, evitando, quindi, di rispondere all'adescatore al suo posto). È fondamentale valutare il benessere psicofisico dei minori e il rischio che corrono. Vi ricordiamo che l'attuale normativa prevede che la persona coinvolta in qualità di vittima o testimone in alcune tipologie di reati, tra cui il grooming, debba essere ascoltata in sede di raccolta di informazioni con l'ausilio di una persona esperta in psicologia o psichiatria infantile.

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

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

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

5.2. - Come segnalare: quali strumenti e a chi

L'insegnante riveste la qualifica di pubblico ufficiale in quanto l'esercizio delle sue funzioni non è circoscritto all'ambito dell'apprendimento, ossia alla sola preparazione e tenuta delle lezioni, alla verifica/valutazione dei contenuti appresi dagli studenti e dalle studentesse, ma si estende a tutte le altre attività educative. Le situazioni problematiche in relazione all'uso delle tecnologie digitali dovrebbero essere sempre gestite anche a livello di gruppo. Come descritto nelle procedure di questa sezione, si potrebbero palesare due casi:

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

Strumenti a disposizione di studenti/esse

Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione:

- un indirizzo e-mail specifico per le segnalazioni;
- scatola/box per la raccolta di segnalazioni anonime da inserire in uno spazio accessibile e ben visibile della scuola;
- sportello di ascolto con professionisti;
- docente referente per le segnalazioni.

Anche studenti e studentesse, inoltre, possono rivolgersi alla Helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96. Il nostro istituto, nel suo interno ha nominato un docente referente per il contrasto al Bullismo e Cyberbullismo a cui i docenti possono rivolgersi per la segnalazione di casi sospetto e valutare insieme le possibili strategie d'intervento. Sarà di valido aiuto un diario di bordo dove poter raccogliere informazioni sul caso sospetto. Inoltre, sempre nel nostro istituto, è attivo uno sportello di ascolto con professionisti dell'ASL pronti a supportare le persone che vivono eventuali situazioni di cyberbullismo. Di fronte ad un caso accertato di cyberbullismo, il docente di classe deve condividere immediatamente di quanto è a conoscenza con il referente di bullismo e cyberbullismo, valutando insieme possibili strategie di intervento. Si

avvisa il Dirigente scolastico che convoca il Consiglio di classe. Se non si ravvisano fattispecie di reato:
- si informano i genitori degli alunni direttamente coinvolti (possibilmente con la presenza dello psicologo);
-- si richiede la consulenza dello psicologo scolastico a supporto della gestione
-informare i genitori degli alunni infra quattordicenni della possibilità di richiedere la rimozione, l'oscuramento o il blocco di contenuti offensivi ai gestori di siti internet o social
-attivare il Consiglio di classe
-valutare come coinvolgere gli operatori scolastici su ciò che sta accadendo.

5.3. - Gli attori sul territorio

Talvolta, nella gestione dei casi, può essere necessario rivolgersi ad altre figure, enti, istituzioni e servizi presenti sul territorio qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.
Per una mappatura degli indirizzi di tali strutture è possibile consultare il Vademecum di Generazioni Connesse "Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all'utilizzo delle tecnologie digitali da parte dei più giovani" (seconda parte, pag. 31), senza dimenticare che la Helpline di Telefono Azzurro (19696) è sempre attiva nell'offrire una guida competente ed un supporto in tale percorso.
A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all'utilizzo di Internet può presentare.

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

- Ufficio Scolastico Regionale: supporta le scuole in attività di prevenzione ed anche nella segnalazione di comportamenti a rischio correlati all'uso di Internet.
- Polizia Postale e delle Comunicazioni: accoglie tutte le segnalazioni relative a comportamenti a rischio nell'utilizzo della Rete e che includono gli estremi del reato.
- Aziende Sanitarie Locali: forniscono supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in Rete.

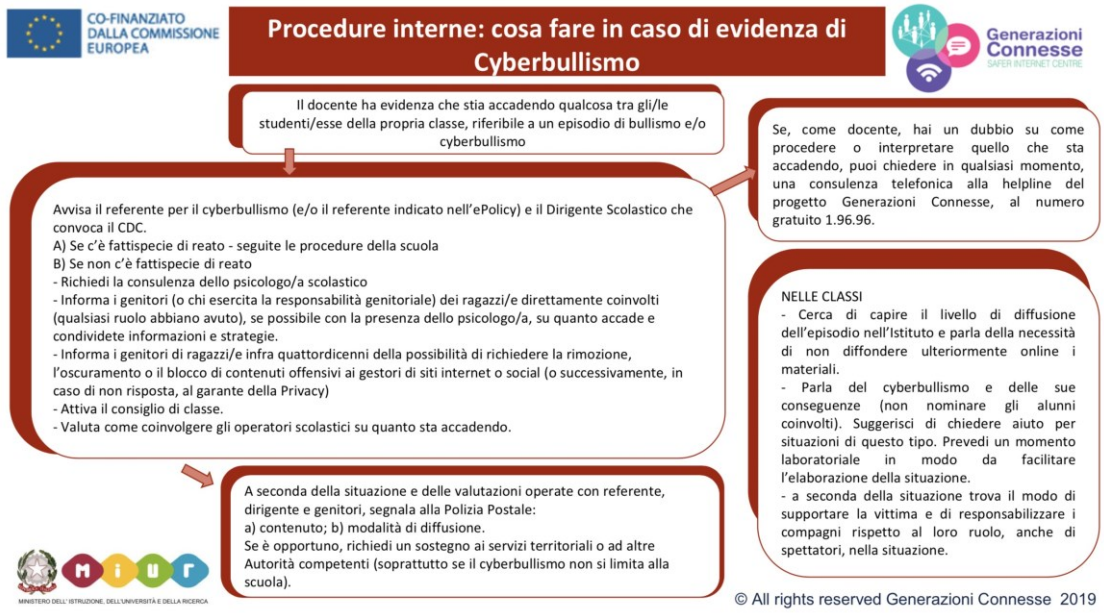
Il Garante Regionale per l'Infanzia e l'Adolescenza e Difensore Civico:

- segnalano all'Autorità Giudiziaria e ai Servizi Sociali competenti;
- accolgono le segnalazioni di presunti abusi e forniscono informazioni sulle modalità di tutela e di esercizio dei diritti dei minori vittime.
- Segnalano alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.

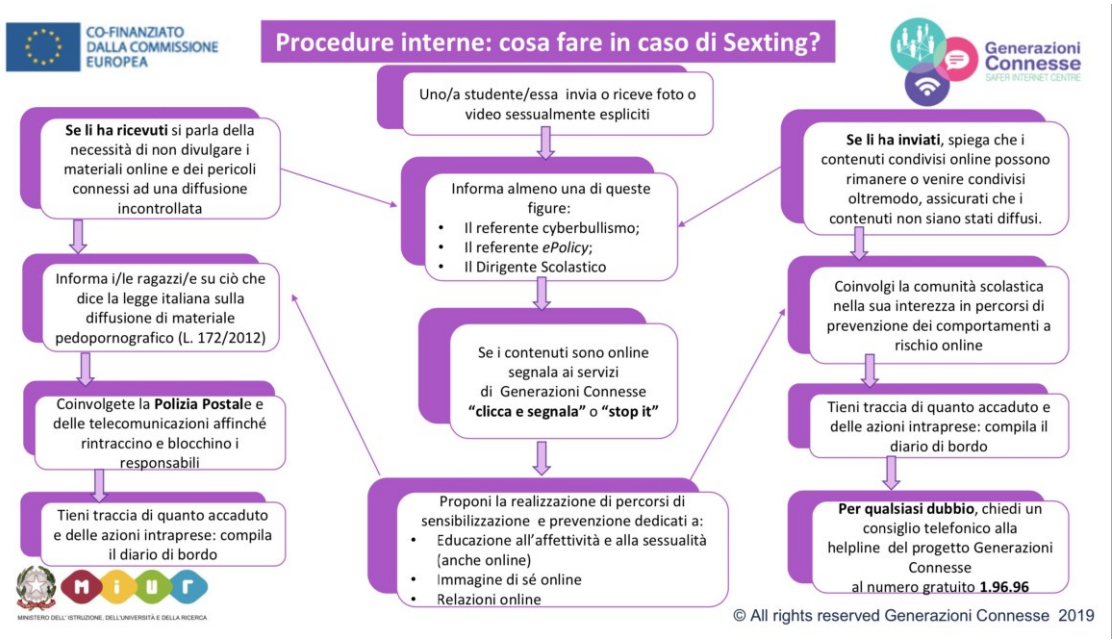
Il Tribunale per i Minorenni: segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

5.4. - Allegati con le procedure

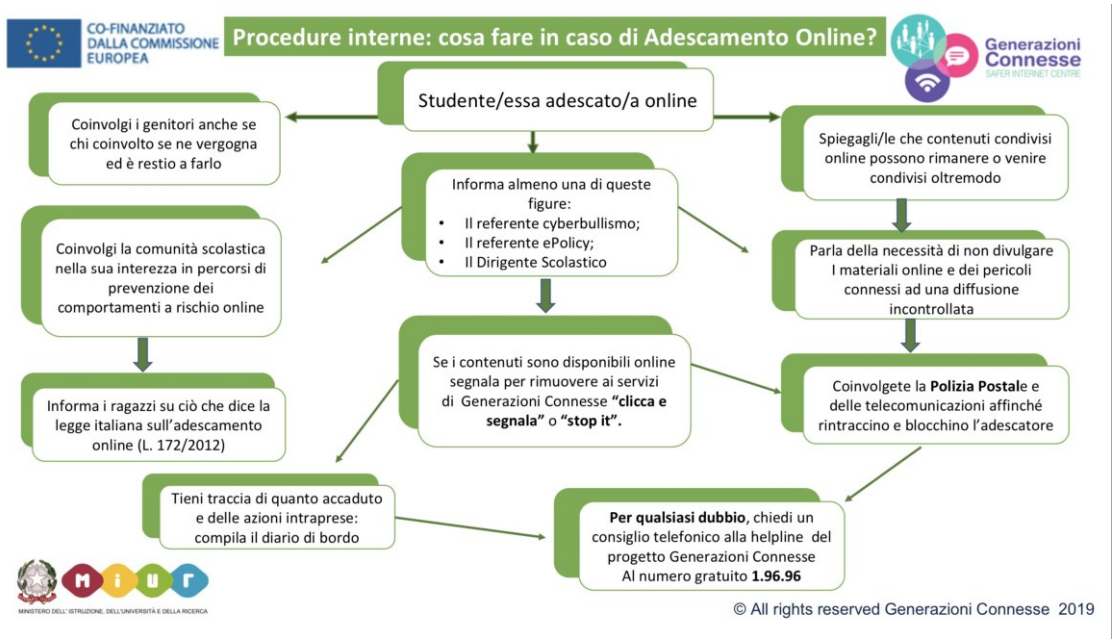
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



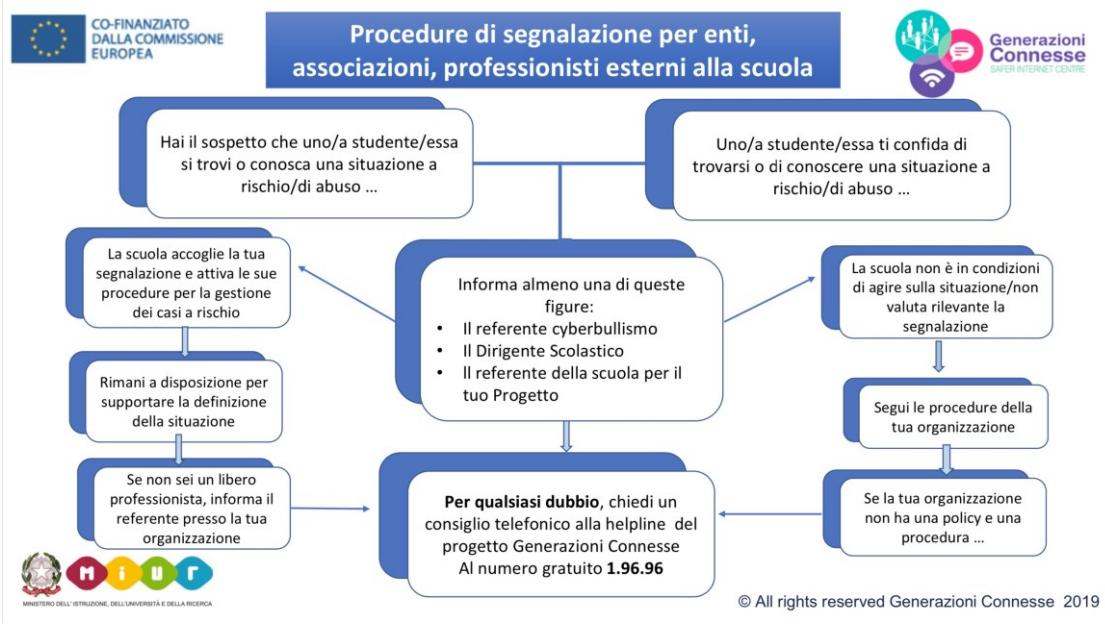
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



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



Altri allegati

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

Modulo di segnalazione di casi

Nome di chi compila la segnalazione: Ruolo:

Data: Scuola:

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

Schema riepilogativo delle situazioni gestite legate a rischi online

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

Il nostro piano d'azioni

- Informare la comunità scolastica sulle figure interne di riferimento per la segnalazione dei casi
-Rendere consapevoli gli studenti dei rischi online anche attraverso una formazione peer to peer
-portare a conoscenza i docenti e le famiglie sulle procedure di segnalazione dei casi che la scuola è tenuta ad adottare in presenza di casi sospetti o accertati di bullismo e cyberbullismo
-promuovere incontri con le famiglie per attenzionarle alle problematiche che i loro figli possono incorrere utilizzando la comunicazione attraverso il web.

Raggiungere il 100% degli studenti
Raggiungere il 100% dei docenti
Raggiungere il 50% delle famiglie

Il Dirigente Scolastico