Documento di ePolicy

CSIC8AT008

IC TORTORA

VIA PROVINCIALE N.37 - 87020 - TORTORA - COSENZA (CS)

GIUSEPPE PEDUTO

Capitolo 1 - Introduzione al documento di ePolicy

1.1 - Scopo dell'ePolicy

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

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

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

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

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

Argomenti del Documento

1. **Presentazione dell'ePolicy**
    1. Scopo dell'ePolicy
    2. Ruoli e responsabilità
    3. Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto
    4. Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica
    5. Gestione delle infrazioni alla ePolicy
    6. Integrazione dell'ePolicy con regolamenti esistenti
    7. Monitoraggio dell'implementazione dell'ePolicy e suo aggiornamento
2. **Formazione e curricolo**
    1. Curricolo sulle competenze digitali per gli studenti
    2. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica
    3. Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali
    4. Sensibilizzazione delle famiglie e Patto di corresponsabilità
3. **Gestione dell'infrastruttura e della strumentazione ICT (Information and Communication Technology) della e nella scuola**
    1. Protezione dei dati personali
    2. Accesso ad Internet
    3. Strumenti di comunicazione online
    4. Strumentazione personale
4. **Rischi on line: conoscere, prevenire e rilevare**
    1. Sensibilizzazione e prevenzione
    2. Cyberbullismo: che cos'è e come prevenirlo
    3. Hate speech: che cos'è e come prevenirlo
    4. Dipendenza da Internet e gioco online
    5. Sexting
    6. Adescamento online
    7. Pedopornografia
5. **Segnalazione e gestione dei casi**
    1. Cosa segnalare
    2. Come segnalare: quali strumenti e a chi
    3. Gli attori sul territorio per intervenire
    4. Allegati con le procedure

Perché è importante dotarsi di una E-policy?

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

all'uso di Internet.

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

La presenza sempre più diffusa delle tecnologie digitali nella vita di tutti i giorni offre nuove e tante possibilità al mondo della scuola, ma questo impone una riflessione sul loro uso efficace, sicuro e consapevole. Lo sviluppo e l'integrazione dell'uso delle TIC, nella didattica, creano le condizioni per una trasformazione dell'insegnamento e dell'apprendimento mettendoci davanti a sfide importanti che riguardano gli stili di apprendimento, i livelli delle conoscenze, le abilità e le competenze che i giovani hanno bisogno di sviluppare verso le competenze digitali.

L'Istituto Comprensivo di Tortora ha colto l'occasione di dotarsi di una Policy di e-safety per essere pronto a cogliere tutti i cambiamenti sociali, economici, culturali e tecnologici di questa nuova società che è in continuo movimento di sviluppo, in modo da contribuire a formare i cittadini di domani destinati a vivere in un ambiente in cui tutto viene sviluppato attraverso l'uso delle nuove tecnologie.

Con questo documento si vuole regolamentare l'uso di Internet per rendere responsabili tutti gli utenti dell'Istituto garantendo la privacy all'interno dei diversi plessi scolastici e degli uffici di segreteria. Le indicazioni Nazionali volgono l'attenzione sulle competenze digitali degli studenti, ai quali è richiesto di sapersi orientare nel Web, scambiando informazioni ed esperienze in modo consapevole e responsabile, per questo occorre formare ed informare tutte le componenti scolastiche sui rischi online, fornendo misure atte a prevenirli, permettendo di beneficiare in sicurezza delle opportunità offerte da Internet e dalle TIC.

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.

Nell'ambito di questa Policy sono individuati ruoli e principali responsabilità correlate:

Dirigente Scolastico:

- garantisce la tutela degli aspetti legali riguardanti la privacy e l'immagine di tutti i membri della comunità scolastica;

- garantisce ai propri docenti una formazione di base sulle Tecnologie dell'Informazione e della Comunicazione tale da consentire di acquisire le competenze necessarie per l'utilizzo delle risorse informatiche;
- garantisce l'esistenza di un sistema di monitoraggio e di controllo interno della sicurezza online e vigila sui comportamenti inadeguati;
- gestisce e interviene nei casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali.

Animatore Digitale:

- rileva i bisogni formativi riguardanti l'uso delle nuove tecnologie;
- supporta i docenti nel familiarizzare con le nuove tecnologie multimediali nella didattica;
- assicura l'accesso alla rete e ai dispositivi della scuola;
- coinvolge l'intera comunità attraverso azioni di informazione e formazione nell'ambito di sviluppo della "scuola digitale".

Referente Bullismo e Cyberbullismo:

- coordina e promuove iniziative specifiche per la prevenzione e il contrasto del Bullismo e Cyberbullismo;
- coinvolge, con progetti studenti, docenti e genitori;
- promuove percorsi formativi con particolare attenzione alla formazione fornita da Generazioni Connesse e dalla piattaforma Elisa;
- coordina il gruppo di lavoro per la stesura o la revisione della ePolicy.

Gruppo di lavoro:

- collabora con il referente Bullismo e Cyberbullismo;
- promuove iniziative e attività di sensibilizzazione nei plessi scolastici di appartenenza;
- partecipa alla stesura e alla revisione del documento di ePolicy.

Docenti:

- diffondono la cultura dell'uso responsabile delle TIC e della rete;
- integrano parti del curricolo della propria disciplina con approfondimenti sulla tematica;
- promuovono l'uso consapevole delle tecnologie digitali nella didattica;
- accompagnano e supportano gli studenti nell'utilizzano della LIM e di tutti gli strumenti tecnologici in dotazione alla scuola;
- segnalano al Dirigente Scolastico e al referente d'istituto Bullismo e Cyberbullismo qualunque problematica che vede coinvolti gli alunni.

Il personale Amministrativo, Tecnico e Ausiliario (ATA):

- svolge funzione di gestione e di sorveglianza connesse all'attività dell'istituzione scolastica, in collaborazione con il dirigente scolastico e con il

personale docente tutto che concerne non solo il tempo scuola e il potenziamento dell'offerta formativa, ma anche le attività di formazione e autoformazione in tema di bullismo e cyberbullismo;
- è coinvolto nella segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo e nella raccolta, verifica e valutazione delle informazioni inerenti possibili casi di bullismo/cyberbullismo.

Gli Studenti e le Studentesse:

- utilizzano, in relazione al proprio grado di maturità e consapevolezza raggiunta, tecnologie digitali in coerenza con quanto richiesto dai docenti;
- il supporto della scuola garantisce la tutela online;
- partecipano attivamente a progetti ed attività che riguardano l'uso positivo delle TIC e della Rete;
- promuovono quanto appreso anche attraverso possibili percorsi di peer education.

I Genitori in linea con l'Istituto scolastico:

- sono partecipi e attivi nelle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete;
- sono responsabili dei device personali dei propri figli;
- si relazionano in modo costruttivo con i docenti sulle linee educative che riguardano le TIC e la Rete;
- comunicano con i docenti circa i problemi rilevati quando i/le propri/e figli/e non usano responsabilmente le tecnologie digitali o Internet.

Gli Enti educativi esterni e le associazioni che entrano in relazione con la scuola:

- si conformano alla politica della stessa riguardo all'uso consapevole della Rete e delle TIC;
- promuovono comportamenti responsabili e la sicurezza online;
- assicurano la protezione degli studenti e delle studentesse durante le attività che si svolgono insieme;
- si attengono a quanto specificato dall'ePolicy con indicazioni e procedure per gli attori esterni.

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).

Il nostro Istituto si avvale della collaborazione di professionisti esterni, in parte selezionate dall'Amministrazione Comunale, per ampliare l'offerta formativa, in particolare per gli alunni con bisogni educativi speciali.

Anche loro sono chiamati a condividere i principi e le regole stabilite dalla presente ePolicy.

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.

Le regole contenute nella Policy:

- sono approvate dal Collegio dei Docenti e dal Consiglio d'Istituto;
- integrano il Regolamento d'Istituto e il PTOF;
- saranno pubblicate sul sito web dell'Istituto;
- saranno comunicate agli alunni e con loro condivise attraverso momenti di discussioni e attività didattiche sulla sicurezza 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.

Infrazioni degli alunni.

I provvedimenti disciplinari da adottare da parte dei consigli di classe o d'interclasse nei confronti degli alunni che abbiano commesso una o più infrazione alla Policy saranno i seguenti:

- richiamo verbale;
- sanzioni estemporanee commisurate alla gravità della violazione commessa e all'età dell'alunno, assegnazione di attività aggiuntive da svolgere a casa su temi di Cittadinanza e Costituzione e Cittadinanza Digitale;
- nota informativa ai genitori o tutori mediante registro elettronico;
- convocazione dei genitori per un colloquio con gli insegnanti;
- convocazione dei genitori con il Dirigente Scolastico;
- sono previsti interventi di carattere educativo di rinforzo dei comportamenti corretti, di consolidamento delle regole sociali di convivenza, la partecipazione attiva e consapevole degli alunni delle classi coinvolte, di prevenzione gestione

positiva dei conflitti, promozione dei rapporti di amicizia e di solidarietà, di promozione, conoscenza e gestione delle emozioni.

Infrazioni del personale scolastico.

Le infrazioni alla policy da parte del personale scolastico riguardano:

- la mancata osservanza delle regole sulla gestione della strumentazione, esponendo al rischio gli alunni;
- la mancata sorveglianza e pronto intervento nel caso di infrazioni da parte degli alunni, causando il danno per la non tempestiva attivazione delle regole.

1.6 - Integrazione dell'ePolicy con Regolamenti esistenti

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

La presente ePolicy integra il Regolamento d'Istituto e il PTOF.

1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

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

Il monitoraggio dell'implementazione della Policy avverrà:

- alla fine di ogni anno scolastico;
- all’inizio di ogni anno scolastico, contestualmente alla revisione del PTOF.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

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

Capitolo 2 - Formazione e curricolo

2.1. Curricolo sulle competenze digitali per gli studenti

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

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

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

Le competenze digitali sono una delle competenze chiave europee, come già evidente nella definizione iniziale delle Raccomandazioni Europee e del Consiglio 18-12-2006 e le Indicazioni nazionali del curricolo. Le competenze digitali richiamano diverse dimensioni sulle quali è possibile lavorare in classe, in un'ottica che integra la dimensione tecnologica con quella cognitiva ed etica (per approfondimenti si rimanda a Calvani, Fini e Ranieri 2009):

- dimensione tecnologica: è importante far riflettere i più giovani sul potenziale delle tecnologie digitali come strumenti per la risoluzione di problemi della vita quotidiana, onde evitare automatismi che abbiano conseguenze incerte, attraverso un'adeguata comprensione della "grammatica" dello strumento.
- dimensione cognitiva: fa riferimento alla capacità di cercare, usare e creare in modo critico le informazioni condivise in Rete, valutandone credibilità e affidabilità.

- dimensione etica e sociale: la dimensione etica fa riferimento alla capacità di gestire in modo sicuro i propri dati personali e quelli altrui, e di usare le tecnologie digitali per scopi eticamente accettabili e nel rispetto degli altri. La dimensione sociale pone l'accento sulle pratiche sociali e sullo sviluppo di particolari abilità socio-comunicative e partecipative per maturare una maggiore consapevolezza sui nostri doveri nei riguardi di coloro con cui comunichiamo online.

Per tali motivi è opportuno fare riferimento ad un framework comune per le competenze digitali e l'educazione ai media degli alunni. I documenti più importanti per progettare e implementare un buon curricolo sulle competenze digitali a cui fare riferimento sono:

- Piano Scuola Digitale (PNSD), in particolar modo il paragrafo 4.2. su "Competenze e contenuti": è il documento di indirizzo del Ministero dell'Istruzione, dell'Università e della Ricerca per il lancio di una strategia complessiva di innovazione della scuola italiana e per un nuovo posizionamento del suo sistema educativo nell'era digitale.
- Sillabo sull'Educazione Civica Digitale: ha lo scopo di inquadrare il corpus di temi e contenuti che sono alla base dello sviluppo di una piena cittadinanza digitale degli studenti attraverso il percorso educativo.
- DigComp 2.1.: "Il quadro di riferimento per le competenze digitali dei cittadini", con otto livelli di padronanza ed esempi di utilizzo.
- Raccomandazione del Consiglio europeo relativa alle competenze chiave per l'apprendimento permanente (C189/9, p. 9): documento in cui vengono specificate le conoscenze, le abilità e gli atteggiamenti essenziali legati a tale competenza.

Il DigComp, in particolare, è diventato un riferimento per lo sviluppo e la pianificazione strategica di iniziative sulle competenze digitali, sia a livello europeo sia nei singoli stati membri dell'Unione.

Il documento prevede:

1. Aree di competenze individuate come facenti parte delle competenze digitali.
2. Descrittori delle competenze e titoli pertinenti a ciascuna area (21 competenze).
3. Livelli di padronanza per ciascuna competenza (i livelli sono 8).
4. Conoscenze, abilità e attitudini applicabili a ciascuna competenza.
5. Esempi di utilizzo sull'applicabilità della competenza per diversi scopi.

Le aree di competenza individuate dal Digcomp sono, nello specifico:

Area 1: Alfabetizzazione e dati

L'area s'inquadra nella dimensione "informazionale" o "cognitiva" delle competenze digitali. Essa è relativa alla capacità di cercare, selezionare, valutare e riprocessare le

informazioni in Rete. Nello specifico, per quest'area si punta a sviluppare in bambini e ragazzi le seguenti competenze:

1. Navigare, ricercare e filtrare dati, informazioni e contenuti digitali;

2. Valutare e gestire dati, informazioni e contenuti digitali;

3. Saper riconoscere e sapersi difendere da contenuti dannosi e pericolosi in Rete (es. app, giochi online, siti non adatti ai minori, materiale pornografico e pedo-pornografico etc.).

Area 2: Comunicazione e collaborazione

Quest'area fa riferimento a quelle competenze volte a riconoscere le giuste ed appropriate modalità per comunicare e relazionarsi online:

1. Saper interagire con gli altri attraverso le tecnologie digitali;

2. Essere consapevoli nella condivisione delle informazioni in Rete;

3. Essere buoni "cittadini digitali";

4. Collaborare adeguatamente con gli altri attraverso le tecnologie digitali;

5. Conoscere le "Netiquette", ovvero le norme di comportamento online;

6. Saper gestire la propria "identità digitale".

Area 3: Creazione di contenuti digitali

Quest'area fa riferimento alle capacità di "valutare le modalità più appropriate per modificare, affinare, migliorare e integrare nuovi contenuti e informazioni specifici per crearne di nuovi e originali" (cfr. DigComp 2.1.). Le specifiche competenze digitali che vanno sviluppate in questo caso sono:

1. Creare e modificare contenuti digitali in diversi formati per esprimersi attraverso mezzi digitali;

2. Modificare, affinare, migliorare e integrare informazioni e contenuti all'interno di un corpus di conoscenze esistente per creare conoscenze e contenuti nuovi, originali e rilevanti;

3. Capire come il copyright e le licenze si applicano ai dati, alle informazioni e ai contenuti digitali.

Area 4: Sicurezza

Quest'area è parte di una dimensione più generale definita come "benessere digitale" che include la necessità di salvaguardare i propri dati personali e rispettare le regole nel trattare i dati altrui. Nello specifico, si punta a sviluppare in bambini e ragazzi le

seguenti competenze:

1. Imparare a proteggere i dispositivi e i contenuti digitali e comprendere i rischi e le minacce presenti negli ambienti digitali. Conoscere le misure di sicurezza e protezione e tenere in debita considerazione l'affidabilità e la privacy;

2. Proteggere i dati personali e la privacy negli ambienti digitali. Capire come utilizzare e condividere informazioni personali proteggendo se stessi e gli altri dai danni.

Comprendere che i servizi digitali hanno un "regolamento sulla privacy" per informare gli utenti sull'utilizzo dei dati personali raccolti;

3. Conoscere ed esercitare i propri diritti in termini di privacy e sicurezza.

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

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

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

La professione docente è complessa e pertanto richiede competenze diverse e integrate, fra queste anche quelle di tipo digitale. Le TIC, possono essere utilizzate dagli insegnanti a integrazione della didattica al fine di progettare, sviluppare, utilizzare, gestire e valutare i processi di insegnamento e apprendimento di tutti gli alunni della classe, anche delle persone con disabilità, in chiave inclusiva.

È su tali premesse che l'Istituto, attraverso il collegio dei docenti, riconosce e favorisce la partecipazione del personale ad iniziative promosse sia direttamente dalla scuola, dalle reti di scuole e dall'amministrazione, sia quelle liberamente scelte dai docenti, anche online, purché restino coerenti con il piano di formazione.

L'uso delle TIC nella didattica non solo può rendere gli apprendimenti motivanti,

coinvolgenti ed inclusivi, ma permette al docente di guidare gli alunni rispetto alla fruizione dei contenuti online, visto che è la modalità naturale di apprendimento al di fuori della scuola. Inoltre, permettono di sviluppare capacità che sono sempre più importanti anche in ambito lavorativo, come il lavoro di gruppo anche a distanza e il confronto fra pari in modalità asincrona.

La competenza digitale, oggi, è imprescindibile per i docenti così come per gli alunni e permette di integrare la didattica con strumenti che la diversificano, la rendono innovativa e in grado di venire incontro ai nuovi stili di apprendimento.

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, alunni 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 e adeguato che abbia come oggetto non solo l'uso responsabile e sicuro della Rete ma anche i rischi legati a quest'ultime.

Formare i docenti 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. Gli alunni 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.

Per tali ragioni, l'Istituto prevede specifici momenti di formazione per gli insegnanti che mettano al centro i temi in oggetto, considerando anche percorsi di autoaggiornamento personali o collettivi, iniziative seminariali con professionisti-esperti interni ed esterni alla scuola, giornate-settimane di approfondimento in accordo con la rete scolastica del territorio USR, Osservatori regionali sul bullismo, scuole Polo, le amministrazioni comunali, i servizi socio-educativi e le associazioni/enti presenti.

I momenti di formazione e aggiornamento sono pensati e creati 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; dall'analisi delle richieste che provengono dagli alunni stessi in modo, da riutilizzarli nel loro lavoro di educatori (attraverso le modalità che il docente indica e ritiene più confacente alla classe) quanto appreso durante la formazione ricevuta.

Cronoprogramma per il prossimo triennio scolastico:

- 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.
- Predisposizione di un'area specifica sul sito dell'Istituto con materiali formativi per gli insegnanti. Nella sezione, verranno messi a disposizione materiali per l'aggiornamento sull'utilizzo consapevole e sicuro di Internet, prevedendo possibilità e modalità di condivisione fra gli insegnanti.
- Sul sito istituzionale della scuola, viene incluso il link e materiali informativi del progetto "Generazioni connesse", www.generazioniconnesse.it dove è possibile trovare ulteriori approfondimenti, spunti aggiornamenti e strumenti didattici utili da usare con gli studenti e le studentesse, per ciascun grado di scuola e il link della Piattaforma Elisa www.piattaformaelisa.it

---

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.

Il nostro Istituto integra, oltre che il regolamento scolastico, anche il "Patto di corresponsabilità", con specifici riferimenti alle tecnologie digitali e all'ePolicy.

Il "Patto di Corresponsabilità" è un documento centrale per ogni istituzione scolastica e per la comunità educante tutta, al fine di creare una maggiore collaborazione e condivisione degli interventi di formazione e di contrasto al bullismo e al cyberbullismo all'interno della comunità educante e punta a "rafforzare il rapporto scuola/famiglia in quanto nasce da una comune assunzione di responsabilità e impegna entrambe le componenti a condividerne i contenuti e a rispettarne gli impegni".

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dei tre anni)

Il nostro piano d'azione:

- regole sull'uso delle tecnologie digitali da parte dei genitori nelle comunicazioni con la scuola e con i docenti: mail, registro elettronico.
- Percorsi di sensibilizzazione e formazione dei genitori su un uso responsabile e costruttivo della Rete in famiglia e a scuola.
- Azioni e strategie per il coinvolgimento delle famiglie: percorsi di sensibilizzazione mediante l'organizzazione di iniziative in cui gli alunni siano protagonisti.

Tutto ciò in continuità anche con l'art. 5 (comma 2) della legge 29 maggio 2017, n.71 "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo" che prevede l'integrazione, oltre che del regolamento scolastico, anche del "Patto di Corresponsabilità", con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari "commisurate alla gravità degli atti compiuti", al fine di meglio

regolamentare l’insieme dei provvedimenti sia di natura disciplinare che di natura educativa e di prevenzione al fenomeno.

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.

L'Istituto Comprensivo di Tortora opera a ogni livello rispettando tutte le normative vigenti in merito alla tutela della privacy. A seguito della DAD prima e della DDI dopo la scuola ha individuato, fra le piattaforme proposte dal Ministero, Gsuite come quella da utilizzare per la didattica in tutti gli ordini scolastici.

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.

Nell’Istituto Comprensivo di Tortora l’utilizzo delle TIC è in continua evoluzione secondo le indicazioni del PNSD.

Ad oggi tutti i plessi scolastici sono connessi a internet e il segnale è distribuito sia da una rete LAN, con un punto rete per ogni aula didattica, sia da una rete WLAN che funziona in modalità wireless. Ogni aula è dotata di una Lim, il relativo computer portatile è custodito in apposite cassette a muro chiuse a chiave e connesse a Internet.

Durante il periodo di sospensione dell’attività didattica in presenza e all’inizio del presente anno scolastico sono stati distribuiti dispositivi digitali in comodato d’uso alle famiglie che necessitavano di un supporto tecnologico.

Gli alunni sono invitati a non rivelare dettagli o informazioni personali di sé o di altre persone come indirizzi e numeri di telefono e in particolare a non condividere con nessuno password personali.

L’accesso a Internet da parte degli alunni può avvenire solo in presenza e con il controllo di un insegnante e per tutti solo per motivi connessi all’attività didattica e alla formazione.

La scuola ha attivato servizi di cloud-computing, in particolare:

- Axios per la gestione del registro elettronico;
- Gsuite per la gestione della DAD e DDI.

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.

L'Istituto Comprensivo di Tortora si è dotato, da parecchi anni, del registro elettronico Axios, che rappresenta un importante canale di comunicazione con le famiglie. Sul registro elettronico nella sezione dedicata alle famiglie è possibile vedere in tempo reale tutta la carriera scolastica del proprio figlio: dati anagrafici, assenze, ritardi, valutazioni. Nella parte dedicata alla classe è possibile visionare: attività svolte, compiti assegnati, materiale condiviso. Inoltre è possibile prenotare colloqui individuali con i docenti della classe.

Tutte le classi utilizzano la piattaforma GSuite, per la gestione della Didattica a Distanza e della Didattica Digitale Integrata. Ogni utente dell'Istituto o operatore esterno autorizzato dispone di un account personale gestito con livelli di protezione differenziati in base all'età e al ruolo svolto all'interno dell'organizzazione.

Il repository della piattaforma è strutturato per cartelle con gli accessi regolamentati al fine di assicurare un'adeguata conservazione e protezione dei dati.

L'Istituto è dotato di un sito web ufficiale www.istitutocomprensivotortora.edu.it gestito dalla segreteria della scuola e dal Dirigente Scolastico, dove è possibile trovare tutte le informazioni utili per tutto il personale scolastico e per alunni e famiglie.

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.

Il nostro Istituto è dotato di un regolamento sull'uso delle TIC a supporto della ePolicy per poter valutare e monitorare tutti gli aspetti legati alla sicurezza nel momento in cui si permette agli alunni e ai docenti l'accesso alla rete tramite i dispositivi della scuola, tramite la rete scolastica e tramite i dispositivi personali nel caso del BYOD (Bring your own device).

Per meglio definire i confini dei due strumenti:

- l'ePolicy è il documento operativo contenete le norme comportamentali e le procedure per l'utilizzo delle TIC in ambiente scolastico, le misure per la prevenzione e quelle per la rilevazione e gestione delle problematiche connesse ad un uso non consapevole delle tecnologie digitali;
- il regolamento sull'uso delle tecnologie riporta alcune regole relative all'uso della strumentazione tecnologica della scuola, degli ambienti dedicati e della strumentazione personale a scuola, nel caso del BYOD, tablet, PC in classe, ma anche regole per quanto riguarda la presenza degli smartphone a scuola, non a supporto delle attività didattiche.

Il regolamento prevede una parte dedicata all'uso di Internet in cui

gli studenti si impegnano a:

- utilizzare la rete nel modo corretto;
- rispettare le consegne dei docenti;
- non scaricare materiali e software senza autorizzazione;
- non utilizzare unità removibili personali senza autorizzazione;
- tenere spento lo smartphone al di fuori delle attività didattiche che ne prevedano il successivo utilizzo, utilizzarlo esclusivamente per svolgere le attività didattiche previste;
- segnalare immediatamente materiali inadeguati ai propri insegnanti.

I docenti si impegnano a:

- utilizzare la rete nel modo corretto;
- non utilizzare device personali se non per uso didattico;
- formare gli studenti all'uso della rete;
- dare consegne chiare e definire gli obiettivi delle attività;
- monitorare l'uso che gli studenti fanno delle tecnologie a scuola.

In Italia, col recepimento del GDPR, l'età minima per l'accesso ai social network è di 14 anni, 13 con il consenso genitoriale per tutti i social statunitensi. La netiquette può essere elaborata per la scuola secondaria di primo grado e in caso di uso diffuso delle tecnologie in classe, anche alla primaria. Le regole valgono anche per i videogiochi online, a cui spesso i bambini accedono prima di avere uno smartphone.

Checklist per la cybersecurity

- Mantenere separate le reti didattica e segreteria: importante per garantire

maggiore sicurezza alle informazioni, gestendo in modo autonomo e con regole differenti le due reti grazie al firewall.

- Aggiornare periodicamente software e Sistema operativo: garantire che il sistema sia aggiornato lo protegge dalle aggressioni esterne e dalle vulnerabilità che emergono nel tempo.
- Definire la programmazione di backup periodici: cioè la copia e messa in sicurezza dei dati del sistema scolastico per prevenire la perdita degli stessi (possibilmente anche una copia offline).
- Garantire formazione adeguata allo staff, incluso il corpo docenti: la formazione deve riguardare la gestione dei dispositivi, la conoscenza delle regole basilari sulla sicurezza.
- Testare regolarmente le possibili vulnerabilità.
- Preparare piani di azione in risposta ai problemi più seri: è importante non dover improvvisare nel momento in cui si verifica un problema serio, ma avere un protocollo di azione.
- Predisporre la disconnessione automatica dei dispositivi, dopo un certo tempo di inutilizzo: se non è previsto uno stand-by, il dispositivo resta accessibile nel caso in cui qualcuno dimentichi di spegnerlo, con il rischio potenziale di accesso da parte di persone non autorizzate.
- Impostare il browser per l'eliminazione dei cookies alla chiusura: in questo modo si evita che qualcuno possa avere accesso ad account altrui senza autorizzazione.
- Definire una policy sulle password: le password devono essere forti: Richiedere password complesse con almeno 8 caratteri con numeri, maiuscole e minuscole e caratteri speciali. Sensibilizzare rispetto al non uso di password facilmente identificabili (nomi dei figli, compleanni, etc.). Non memorizzare le password nei dispositivi scolastici. Non condividere le password con nessuno.
- Minimizzare i privilegi amministrativi: solo poche persone autorizzate dovrebbero avere privilegi amministrativi. Studenti e la maggior parte dei docenti possono accedere con account con permessi limitati.
- Sviluppare il regolamento sull'uso delle tecnologie a scuola (policy di uso accettabile): deve riguardare chiunque abbia accesso alla Rete, studenti/esse, docenti, amministrazione e segreteria, includere i dispositivi della scuola e quelli personali, anche in caso di BYOD.

Il nostro piano d'azioni

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

- Organizzare uno o più eventi o attività volti a consultare i docenti

dell'Istituto per integrare indicazioni/regolamenti sull'uso dei dispositivi personali a scuola;

- organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali;
- organizzare uno o più eventi o attività volti a formare gli alunni dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali;
- organizzare uno o più eventi o attività volti a formare i genitori dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali.

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

4.1 - Sensibilizzazione e Prevenzione

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

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

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

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

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

La sensibilizzazione è il primo passo verso un cambiamento positivo, ma per far sì che l'intervento sia efficace, è importante che sia chiara l'azione verso cui i soggetti devono impegnarsi.

Due sono gli aspetti da tenere in considerazione:

- la consapevolezza dello status quo;
- la motivazione al cambiamento.

L' intervento di sensibilizzazione prevede i seguenti aspetti:

- spingere le persone a desiderare un cambiamento;
- porre in evidenza la possibilità di generare un cambiamento;
- individuare le azioni che consentono di produrre il cambiamento.

L'attività di sensibilizzazione fornisce le informazioni necessarie e le possibili soluzioni o comportamenti da adottare.

La nostra scuola prevede incontri di sensibilizzazione e si propone di strutturare percorsi di prevenzione rispetto alle tematiche legate ai rischi della rete, con particolare attenzione ai percorsi di prevenzione universale.

Prevenzione Universale. Un programma di questo tipo parte dal presupposto che tutti gli studenti siano potenzialmente a rischio. Si tratta quindi di interventi diretti al grande pubblico o a un intero gruppo di una popolazione che non è stato identificato sulla base del rischio individuale. Efficacia: trattandosi di programmi ad ampio raggio gli effetti di questi programmi possono essere modesti se confrontati con programmi che "trattano" un gruppo con un problema specifico.

I contenuti possono essere adattati più efficacemente in funzione dell'età.

L'approccio prescelto è quello curriculare: le tematiche sono proposte attraverso stimoli letterari, audiovisivi e di attualità.

Le tecniche di rielaborazione sono le seguenti:

- letture e discussioni guidate;
- scrittura e narrazione creativa;
- brainstrorming;
- roleplay.

4.2 - Cyberbullismo: che cos'è e come prevenirlo

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

"qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via

telematica, nonché la diffusione di contenuti on line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo".

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

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

Il cyberbullismo è una forma di prepotenza virtuale messa in atto attraverso l'uso di Internet e delle tecnologie digitali.

Come il Bullismo tradizionale è una forma di prevaricazione e di oppressione reiterata nel tempo, perpetuata da una persona o da un gruppo di persone più potenti nei confronti di un'altra persona percepita come più debole. Le caratteristiche tipiche del bullismo sono l'intenzionalità, la persistenza nel tempo, l'asimmetria di potere e la natura sociale del fenomeno (Olweus, 1996) ma nel Cyberbullismo intervengono anche altri elementi, quali:

- L'impatto: la diffusione di materiale tramite Internet è incontrollabile e non è possibile prevederne i limiti (anche se la situazione migliora, video e immagini potrebbero restare online e continuare a diffondersi).
- La convinzione dell'anonimato: chi offende online potrebbe tentare di rimanere nascosto dietro un nickname e cercare di non essere identificabile.

- L'assenza di confini spaziali: il cyberbullismo può avvenire ovunque, invadendo anche gli spazi personali e privando l'individuo dei suoi spazi-rifugio.
- L'assenza di limiti temporali: può avvenire a ogni ora del giorno e della notte.
- L'indebolimento dell'empatia: quando le interazioni avvengono prevalentemente online la funzione speciale dei neuroni specchio viene meno. La riduzione di empatia che ne consegue può degenerare nei comportamenti noti messi in atto dai cyberbulli.
- Il feedback non tangibile: il cyberbullo non vede in modo diretto le reazioni della vittima e, ancora una volta, ciò riduce fortemente l'empatia e il riconoscimento del danno provocato.

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

Per questo il fenomeno viene talvolta sottovalutato anche dal mondo adulto, familiare e scolastico.

La mediazione tecnologica, infatti, porta ad un certo distanziamento fra aggressore e vittima, causando quello che Bandura ha definito come "disimpegno morale". Si tratta di un indebolimento del controllo morale interno dell'individuo, con la conseguente minimizzazione delle responsabilità individuali. Tale fenomeno vale non solo per il cyberbullo, ma anche per i cosiddetti bystander, ossia coloro che sono spettatori dei fatti.

A ciò si aggiungono altre convinzioni o tendenze frequenti nell'uso della Rete sia da parte dei giovani che degli adulti:

- Percezione che online non ci siano norme sociali da rispettare: fra i giovani spesso vige la falsa convinzione secondo cui la Rete sia uno spazio virtuale lontano dalla realtà, in cui vige libertà assoluta e in cui regole e norme sociali della vita quotidiana non valgono;
- la sperimentazione online di identità e personalità multiple: la Rete è per i minori il luogo virtuale per eccellenza in cui mettersi in gioco "fingendo di essere ciò che non si è" per il semplice gusto di sperimentare nuove forme di identità e comportamento;
- il contesto virtuale come un luogo di simulazione e giochi di ruolo: "la vita sullo schermo" e tutti i comportamenti messi in atto online vengono percepiti solo come un gioco;
- diffusione di responsabilità: tutti quelli che partecipano anche solo con un like o un commento diventano, di fatto, corresponsabili delle azioni del cyberbullo facendo accrescere la portata dell'azione; mettere un "like" su un social network commentare o condividere una foto o un video che prende di mira

qualcuno o semplicemente tacere pur sapendo, mette ragazzi e ragazze nella condizione di avere una responsabilità.

Ma d'altro canto sono proprio loro che possono "fare la differenza" perché la responsabilità è condivisa: il gruppo "silente" che partecipa senza assumersi la responsabilità, rappresenta, in realtà, anche l'elemento che può fermare una situazione di cyberbullismo. E questo appunto costituisce un gancio educativo.

È possibile suddividere gli atti di cyberbullismo in due grandi gruppi:

- cyberbullismo diretto: il bullo utilizza strumenti di messaggistica istantanea (es. sms, messaggi whatsapp) che hanno un effetto immediato sulla vittima, poiché diretti esclusivamente a lei.
- cyberbullismo indiretto: il bullo fa uso di spazi pubblici della Rete (es. social network, blog, forum) per diffondere contenuti dannosi e diffamatori per la vittima. Tali contenuti possono diventare virali e quindi più pericolosi per la vittima anche da un punto di vista psicologico.

È molto importante sottolineare come il cyberbullismo non sia una problematica che riguarda unicamente vittima e cyberbullo. È un fenomeno sociale e di gruppo. Infatti, centrale è il ruolo delle agenzie educative e di socializzazione (formali e informali) più importanti per gli adolescenti: la famiglia, la scuola, i media, le tecnologie digitali e il gruppo dei pari.

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.

L'Istituto Comprensivo di Tortora favorisce la costruzione di una modalità d'intervento non ostile e non basata su stereotipi offensivi. Ogni docente, all'interno delle proprie discipline, dedica del tempo e delle energie alla costruzione di un ascolto attivo e di un dialogo costruttivo.

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?

Il nostro Istituto contribuisce al benessere digitale attraverso azioni di prevenzione che riguardano: la ricerca di un equilibrio tra relazioni online, l'uso degli strumenti digitali per il raggiungimento di obiettivi personali, la capacità di interagire negli ambienti digitali in modo sicuro e responsabile, gestire le distrazioni e il sovraccarico di informazioni, stabilire regole semplici e chiare.

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.

Tra le caratteristiche del fenomeno vi sono principalmente:

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

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

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

4.6 - Adescamento online

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

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

Il miglior modo per prevenire casi di adescamento online è accompagnare ragazze e ragazzi in un percorso di educazione (anche digitale) all'affettività e alla sessualità. Ciò aiuterebbe a renderli più sicuri emotivamente e pronti ad affrontare eventuali situazioni a rischio, imparando innanzitutto a gestire le proprie emozioni, il rapporto con il proprio corpo e con gli altri. È molto importante, inoltre, che ragazzi e ragazze sappiano a chi rivolgersi in caso di problemi, anche quando pensano di aver fatto un errore, si vergognano o si sentono in colpa. Gli adulti coinvolti, genitori e docenti, devono essere un punto di riferimento per il minore che deve potersi fidare di loro e non sentirsi mai giudicato, ma compreso e ascoltato. Affinché ciò avvenga è necessario tenere sempre aperto un canale di comunicazione con loro sui temi dell'affettività.

Nella società digitale, attraverso la Rete, i minori definiscono se stessi, si raccontano e sperimentano nuove forme di identità, socializzano, si emozionano e si relazionano con gli altri.

Tutto ciò risponde a bisogni assolutamente naturali e importanti, ma allo stesso tempo può esporre i ragazzi a possibili rischi come quello dell'adescamento online.

Il desiderio di conferma sociale e, talvolta, la scarsa consapevolezza degli adolescenti nel gestire la propria immagine online quando pubblicano sui loro profili social video e foto, può aumentare il rischio di esporli ad un adescamento online.

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

Come intervenire

Se si sospetta o si ha la certezza di un caso di adescamento online è importante, innanzitutto, che l'adulto di riferimento non si sostituisca al minore nel rispondere, ad

esempio, all'adescatore. È importante che il computer o altri dispositivi elettronici del minore vittima non vengano usati per non compromettere eventuali prove.

Casi di adescamento online richiedono l'intervento della Polizia Postale e delle Comunicazioni a cui bisogna rivolgersi il prima possibile, tenendo traccia degli scambi fra il minore e l'adescatore (ad esempio, salvando le conversazioni attraverso screenshot, memorizzando eventuali immagini o video…).

L'adescamento, inoltre, può essere una problematica molto delicata da gestire e può avere ripercussioni psicologiche significative sul minore. Per questo potrebbe essere necessario rivolgersi ad un Servizio territoriale (es. Consultorio Familiare, Servizio di Neuropsichiatria Infantile, ecc.) in grado di fornire alla vittima anche un adeguato supporto di tipo psicologico o psichiatrico.

Per consigli e per un supporto è possibile rivolgersi alla Helpline di Generazioni Connesse (19696): operatori esperti e preparati sono sempre a disposizione degli insegnanti, del Dirigente e degli operatori scolastici, oltre che dei bambini, degli adolescenti, dei genitori e di altri adulti che a vario titolo necessitano di un confronto e di un aiuto per gestire nel modo più opportuno eventuali esperienze negative e/o problematiche inerenti l'utilizzo dei nuovi media.

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.

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.

Se si è a conoscenza di tale tipologia di reato è possibile far riferimento alla: Polizia di Stato – Compartimento di Polizia postale e delle Comunicazioni; Polizia di Stato – Questura o Commissariato di P.S. del territorio di competenza; Arma dei Carabinieri – Comando Provinciale o Stazione del territorio di competenza; Polizia di Stato – Commissariato online.

Studi in materia dimostrano come l'utilizzo di materiale pedopornografico possa essere propedeutico all'abuso sessuale agito ed è quindi fondamentale, in termini preventivi, intervenire per ridurre l'incidenza di tale possibilità.

L'abuso sessuale online rappresenta una particolare declinazione dell'abuso sessuale su bambini/e, ragazzi/e, la cui caratteristica fondante è il ruolo ricoperto dalle tecnologie digitali, le quali diventano il mezzo principale attraverso cui l'abuso viene perpetrato, documentato e diffuso in Rete con immagini e/o video. Le dinamiche attraverso cui l'abuso sessuale online si manifesta producono effetti sulle vittime che si

aggiungono e moltiplicano a quelli associati all'abuso sessuale. Negli ultimi anni, infine, abbiamo assistito all'emergere di un altro fenomeno che può avere risvolti connessi al fenomeno della pedopornografia: il sexting. La mancanza di intenzione di danneggiare o sfruttare l'altro/a (anche se a volte tale materiale può essere successivamente utilizzato con questo scopo come nel caso del cyberbullismo o del ricatto a fini di estorsione) non esclude che i comportamenti del sexting possano configurare reati connessi con la pedopornografia poiché, secondo il nostro ordinamento giudiziario, il materiale così prodotto e scambiato si declina come pedopornografico e soprattutto perché il rischio di perdere il controllo di tali immagini, uscendo dallo scambio consensuale è molto alto e spesso ragazzi e ragazze non hanno consapevolezza delle conseguenze (anche serie) delle loro azioni, come la possibilità di diffondere in Rete immagini intime/private di altri/e fuori dai canali riservati dello scambio.

Secondo il recente parere emesso del Comitato di Lanzarote del Consiglio d'Europa (l'organismo incaricato di monitorare l'attuazione della Convenzione del Consiglio d'Europa sulla protezione dei/lle bambini/e contro lo sfruttamento e gli abusi sessuali), il "sexting" tra minori (generare, ricevere e condividere in modo consensuale immagini/video a sfondo sessuale o sessualmente espliciti di sé stessi attraverso le tecnologie digitali) non costituisce una condotta connessa alla "pedopornografia", se destinato esclusivamente all'uso privato dei minori, tuttavia se il materiale privato dovesse essere diffuso si configurerebbe invece come pedopornografico. Il parere specifica inoltre che i minori costretti a tale condotta dovrebbero essere affidati ai servizi di assistenza alle vittime e non essere perseguiti penalmente e che particolare attenzione andrebbe posta, nel caso tale materiale fosse prodotto tra bambini/e.

I più giovani devono acquisire quelle competenze in grado di orientarli e guidarli nelle loro scelte anche online; per questo motivo, l'educazione, compresa l'educazione all'affettività, riveste un ruolo fondamentale.

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. Risulta utilissima l'attività educativa sull'affettività e le relazioni, sottolineando sempre la necessità di rivolgersi ad un adulto quando qualcosa online mette a disagio.

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

Inoltre, è auspicabile che possa rientrare nei temi di un'attività di sensibilizzazione rivolta ai genitori e al personale scolastico, promuovendo i servizi delle hotline. Per maggiori approfondimenti, si fa riferimento al Vademecum di Generazioni Connesse.

Il nostro piano d'azioni

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

- Promuovere incontri e laboratori per gli alunni dedicati all'Educazione Civica Digitale.
- Organizzare incontri per la promozione del rispetto delle diversità.
- Organizzare laboratori di educazione all'affettività.
- Organizzare incontri di sensibilizzazione sui rischi online.
- Organizzare incontri per un utilizzo sicuro e consapevole delle tecnologie digitali.
- Organizzare incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali.
- Organizzare incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie rivolto ai genitori e ai docenti.
- Organizzare eventi e dibattiti sui temi della diversità e sull'inclusione rivolti agli alunni, ai docenti e ai genitori.
- Pianificare e realizzare progetti di peer-education sui temi della sicurezza online nella scuola.
- Organizzare incontri rivolti ai genitori sui rischi inerenti la dipendenza da Internet e gioco online, sexting, adescamento online, pedopornografia.

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.

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

Strumenti a disposizione di studenti/esse

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

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

Anche studenti e studentesse, inoltre, possono rivolgersi alla Helpline del progetto

Generazioni Connesse, al numero gratuito 1.96.96.

La scuola mette a disposizione indirizzi email e contatti telefonici affissi in ogni plesso scolastico delle figure di riferimento:

- Dirigente Scolastico prof. Giuseppe Peduto;
- docente Barbara Maria Valente referente d'istituto Bullismo e Cyberbullismo, coordinatrice delle segnalazioni, della gestione dei casi e referente per i genitori.
- docente Antonietta Anna Napolitano per il plesso "P. Cavaliere;
- docente Caterina Senatore per il plesso "G. Cunto;
- docente Concetta Capua per il plesso "T. Sagario";
- docente Claudia Sarubbo per il plesso "A. Fulco";
- docente Pasqule Bianco animatore digitale;
- psicologa nomita dall'istituto scolastico.

5.3. - Gli attori sul territorio

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

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

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

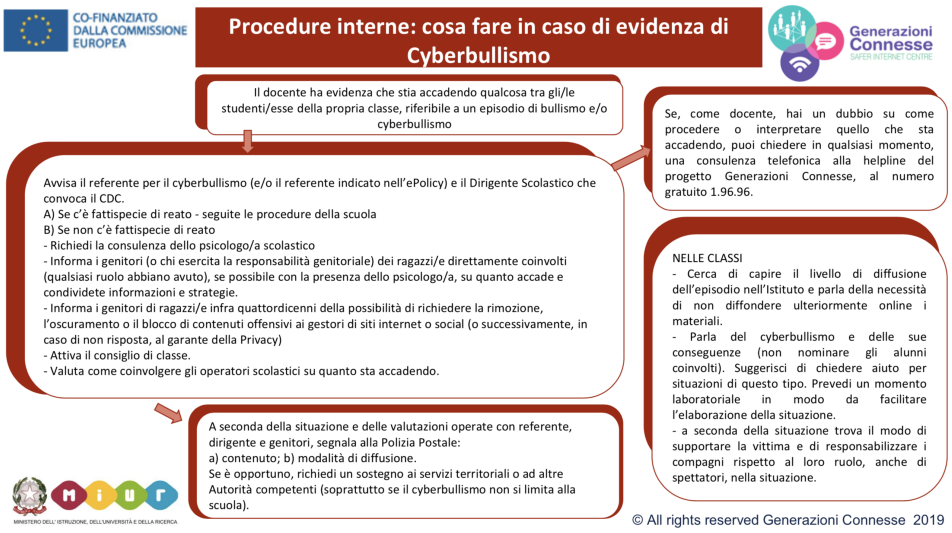
- **Comitato Regionale Unicef**: laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell’infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni)**: svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con

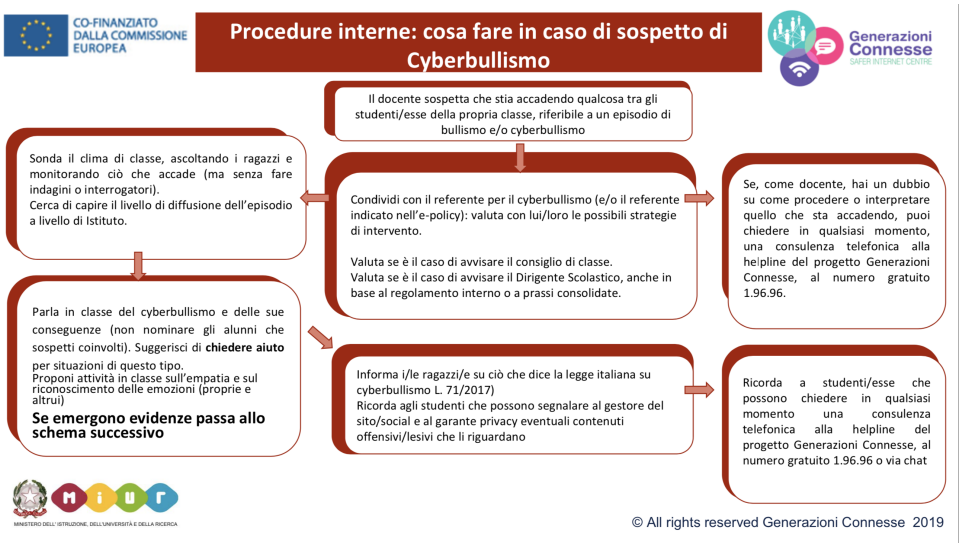
particolare attenzione alla tutela dei minori.

- **Ufficio Scolastico Regionale**: supporta le scuole in attività di prevenzione ed anche nella segnalazione di comportamenti a rischio correlati all'uso di Internet.
- **Polizia Postale e delle Comunicazioni**: accoglie tutte le segnalazioni relative a comportamenti a rischio nell'utilizzo della Rete e che includono gli estremi del reato.
- **Aziende Sanitarie Locali**: forniscono supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in Rete. In alcune regioni, come il Lazio e la Lombardia, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da Internet e alle situazioni di rischio correlate.
- **Garante Regionale per l'Infanzia e l'Adolescenza e Difensore Civico**: segnalano all'Autorità Giudiziaria e ai Servizi Sociali competenti; accolgono le segnalazioni di presunti abusi e forniscono informazioni sulle modalità di tutela e di esercizio dei diritti dei minori vittime. Segnalano alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.
- **Tribunale per i Minorenni**: segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

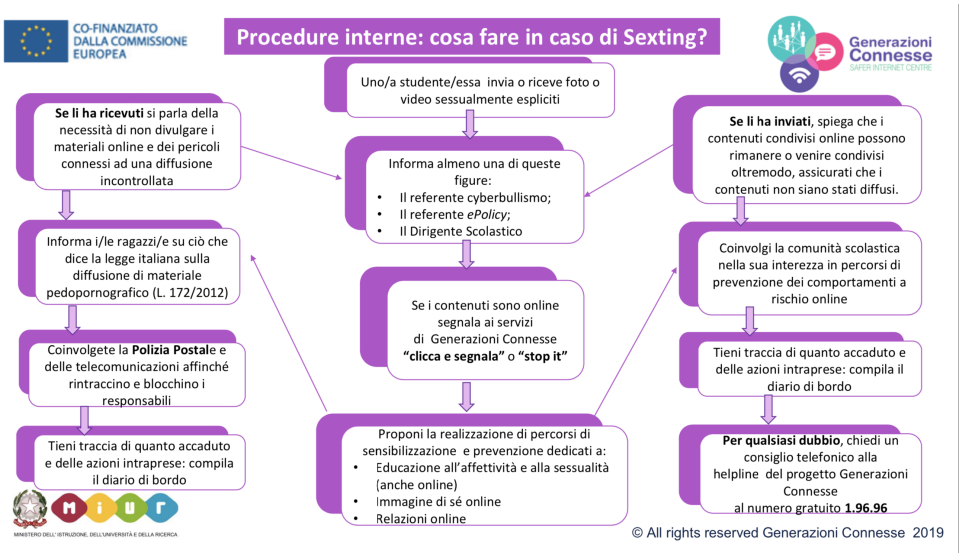
5.4. - Allegati con le procedure

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

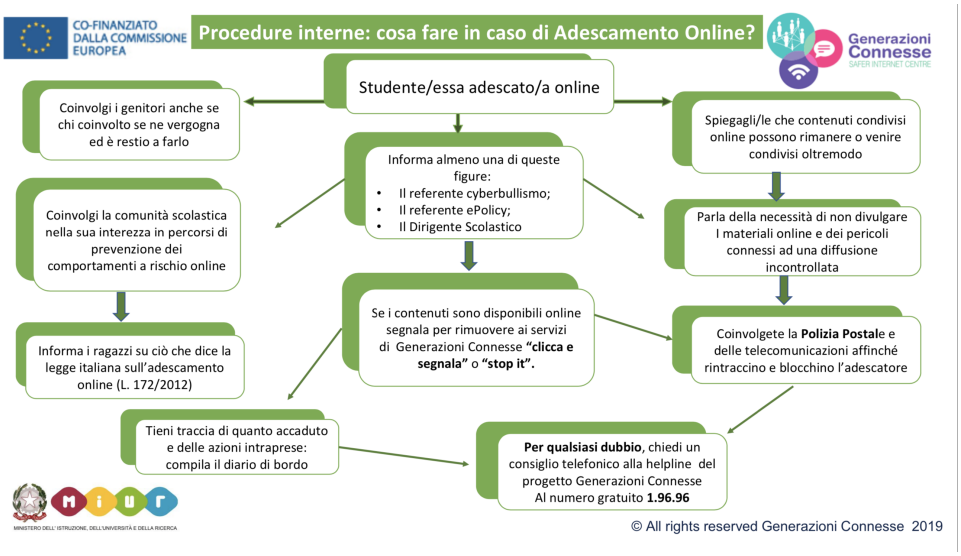




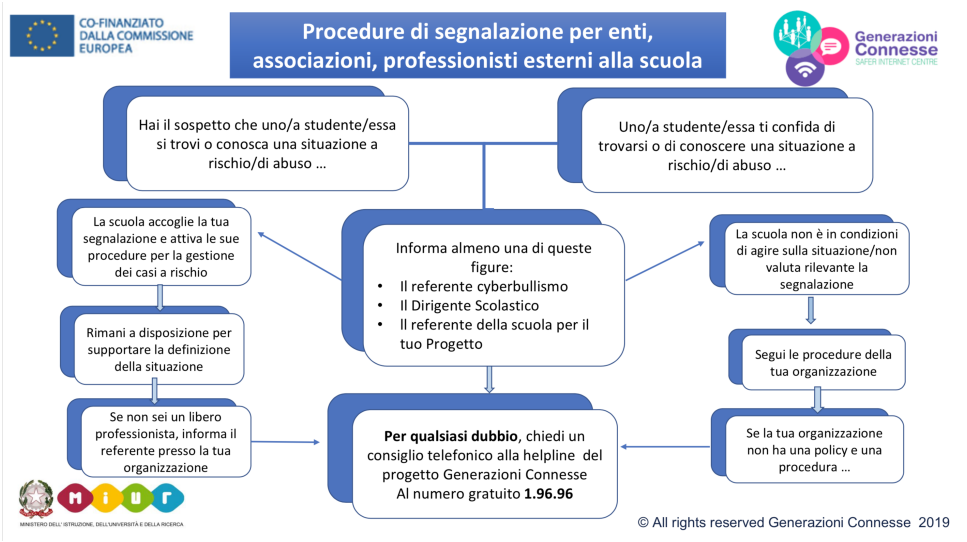
Procedure interne: cosa fare in caso di sexting?



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

Tutte le mappe per le procedure interne vengono stampate, plastificate e affissi in tutti i plessi scolastici.

Le schede per le segnalazioni e il diario di bordo vengono messe a disposizione per tutti i docenti.

Il nostro piano d'azioni

Si considerano da segnalare tutte quelle situazioni caratterizzate da volontarie e ripetute aggressioni mirate a insultare, minacciare, diffamare o ferire una persona o un piccolo gruppo tramite un utilizzo irresponsabile e improprio delle tecnologie digitali.

In particolare si segnaleranno:

- contenuti afferenti la violazione della privacy, informazioni private proprie o degli amici, foto, video pubblicati contro la propria volontà.
- Contenuti afferenti all'aggressività o alla violenza, messaggi minacciosi, commenti offensivi, pettegolezzi, informazioni false, foto, video, virus, contenuti razzisti, immagini o video umilianti, insulti, videogiochi per adulti.
- Contenuti afferenti alla sessualità.

I docenti provvedono a registrare su apposite schede le segnalazioni e a conservare tutte le prove in loro possesso sulla condotta scorretta o dell'abuso rilevati sui pc della scuola. Per le violazioni, minacce o persecuzioni sui telefoni cellulari si può assicurare che l'alunno vittima salvi ogni messaggio conservando così il numero del mittente.

Conservare la prova è utile per far conoscere l'accaduto ai genitori, qualora non si disponga di prove, ma solo di testimonianze dell'alunno, anche accadute al di fuori del contesto scolastico, le notizie sono comunque comunicate ai genitori e i fatti rilevanti anche al Dirigente Scolastico e al referente d'Istituto per il Bullismo e il Cyberbullismo per poter meglio organizzare interventi mirati.

Le procedure interne per la rilevazione e gestione dei casi, la segnalazione al Dirigente Scolastico e al referente d'Istituto Bullismo e Cyberbullismo, avvengono secondo i protocolli suggeriti dalla piattaforma messa a disposizione da "Generazioni Connesse" e dalla Piattaforma Elisa.

Ogni azione programmata è volta a promuovere:

- incontri di teem per perfezionare le procedure;
- promuovere in tutta la comunità scolastica la diffusione delle conoscenze circa le procedure e le figure di riferimento;
- promuovere incontri e laboratori per gli alunni dedicati alle tematiche in oggetto;
- organizzare incontri formativi rivolti alle famiglie sulle segnalazioni, le procedure e gli attori del territorio.
- Incoraggiare il personale scolastico a intraprendere corsi di formazione per conoscere e prevenire il Bullismo e il Cyberbullismo dentro e fuori l'ambiente scolastico.

Referente d'Istituto Bullismo e Cyberbullismo

Ins. Valente Barbara Maria

Gruppo di lavoro

Ins. Napolitano Antonietta Anna (Plesso "P. Cavaliere")

Ins. Senatore Caterina (Plesso "G. Cunto")

Ins. Capua Concetta (Plesso "T. Sagario")

Prof.ssa Sarubbo Claudia (Plesso "A. Fulco")

Firmato da:
PEDUTO GIUSEPPE
Codice fiscale: PDTGPP81P20H703X
19/05/2021 12:18:07