Documento di ePolicy

FGIC82900Q

I.C. "DON MILANI UNO+MAIORANO"

VIA COPPA DEL VENTO 3 - 71043 - MANFREDONIA - FOGGIA (FG)

Miriam Totaro

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

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.

Attraverso l'E-policy lil 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.
Infatti, Le TIC e l'accesso a Internet dal computer di classe o dai dispositivi personali, pur configurandosi come strumenti atti a favorire l'apprendimento, possono, se utilizzati in modo improprio, costituire fattori di rischio tanto per gli studenti, quanto per gli adulti, "immigrati digitali", che intervengono a vario titolo nel processo educativo. Si ritiene pertanto necessario sviluppare un approccio organico alle tematiche legate alle competenze digitali, alla sicurezza online e ad un uso consapevole delle tecnologie digitali nella didattica, stabilendo norme comportamentali e procedure per l'utilizzo delle tecnologie digitali in ambiente scolastico e individuando misure per la prevenzione, per la rilevazione e gestione delle problematiche connesse ad un uso non consapevole delle tecnologie digitali.
L'E- policy fornisce quindi, delle linee guida per garantire il benessere in Rete, definendo le regole dell'utilizzo delle TIC a scuola e ponendo le basi per azioni formative e educative su e con le tecnologia digitali, oltre che sensibilizzare su un uso consapevole delle stesse. Il nostro Istituto, quindi, 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.

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 e-Policy sono individuati i seguenti ruoli e le

principali responsabilità correlate. IL DIRIGENTE SCOLASTICO
E' garante della sicurezza, anche online, di tutti i membri della comunità scolastica, promuove la cultura della sicurezza anche online della intera comunità scolastica, tutelandone i dati. . Attiva, promuove e organizza con la collaborazione del Referente di Istituto per il bullismo e il cyberbullismo percorsi di formazione sull'uso delle TIC , sulla sicurezza e sulle problematiche connesse all'utilizzo della Rete. Gestisce l'esistenza di un sistema e di un protocollo per il monitoraggio e il controllo della sicurezza online. Interviene nella gestione e di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali da parte degli studenti e delle studentesse.

L'ANIMATORE DIGITALE
Supporta il personale scolastico da un punto di vista non solo tecnico-informatico, ma anche in riferimento ai rischi online, alla protezione e gestione dei dati personali ,promuove corsi di formazione sull'uso appropriato delle TIC .Monitora e rileva eventuali episodi o problematiche connesse all'uso delle TIC a scuola.

IL REFERENTE BULLISMO E CYBERBULLISMO
Coordina e promuove iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo. Monitora eventuali azioni di cyberbullismo, ha il compito di diffondere l'e-Policy, coordina e promuove iniziative specifiche per la prevenzione e il contrasto del bullismo e cyberbullismo, avvalendosi anche delle Forze di Polizia, delle associazioni e degli enti territoriali.
I DOCENTI
Integrano parti del curricolo con approfondimenti sull'uso responsabile delle TIC e della Rete. Sviluppano le
competenze digitali degli allievi facendo in modo che conoscano e seguano le norme di sicurezza
nell'utilizzo del web. Segnalano alle famiglie eventuali problematiche emerse in classe nell'utilizzo del digitale e stabiliscono linee comuni di intervento educativo. Responsabilizzano gli alunni relativamente ai problemi legali dei contenuti elettronici come ad esempio siti illegali, plagio, leggi sul copyright e relativi problemi di sicurezza online; promuovono e diffondono il regolamento relativo al corretto utilizzo a scuola dei dispositivi elettronici: cellulari, fotocamere, dispositivi portatili; osservano, valutano e segnalano qualsiasi abuso, sospetto o problema ai responsabili della sicurezza online e al D. S, per le opportune indagini/azioni/ sanzioni;
IL PERSONALE ATA
Svolge funzioni di gestione e sorveglianza , in collaborazione con il Dirigente scolastico e il personale docente. Segnala al Dirigente

scolastico e ai suoi collaboratori episodi di bullismo o cyberbullismo
GLI ALUNNI
Rispettano le norme che disciplinano l'uso corretto e responsabile delle tecnologie digitali adottando le regole di e-safety per evitare situazioni di rischio per sé e per gli altri. informano immediatamente il docente di qualsiasi abuso e/o messaggio, informazione o pagina che compare sul dispositivo utilizzato che crea disagio; sono consapevoli dei rischi e delle conseguenze, anche penali, per un uso non corretto di Internet e delle altre tecnologie, sia a scuola che a casa
I GENITORI
Partecipano alle iniziative di sensibilizzazione e formazione organizzate dall'Istituto sul tema dell'uso consapevole della Rete e dei device personali. Conoscono il Regolamento di Istituto e i relativi provvedimenti disciplinari

GLI ENTI EDUCATIVI ESTERNI E LE ASSOCIAZIONI
Gli enti educativi esterni e le associazioni partecipano al processo educativo , condividendone le regole
relative all'uso consapevole della Rete e delle TIC.
Attivano procedure e comportamenti sicuri per la protezione degli studenti e delle studentesse durante le attività che vengono svolte all'interno della scuola o in cui sono impegnati gli stessi.

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).

La dirigenza e le figure da lei individuate redigono un'apposita informativa per i professionisti esterni che specifica ambiti di applicazione, codice di comportamento, procedure di segnalazione e provvedimenti nel caso di omessa segnalazione o violazione del codice di comportamento. Le figure professionali e le organizzazioni coinvolte in progetti, laboratori e attività devono prendere visione di tutti i documenti proposti dall'Istituto e sottoscriverli preliminarmente all'avvio dei programmi con gli studenti e le studentesse, in classe o fuori

---

1.4 - Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica

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

L'ePolicy d'Istituto viene condivisa a tutta la comunità scolastica attraverso la sua pubblicazione sul sito della scuola, nel PTOF , nel

Regolamento di Istituto. Verrà esposta agli alunni delle classi prime durante i primi giorni di scuola nelle attività di accoglienza e sarà esposto ai genitori all'inizio dell'anno scolastico , allegata al Patto di corresponsabilità.

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.

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. Nel caso in cui vengano violate norme presenti nel Regolamento dell'Istituto 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, anche con l'eventuale intervento di enti esterni.

1.6 - Integrazione dell'ePolicy con Regolamenti esistenti

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

Il presente regolamento sarà inserito nel PTOF , nel Regolamento di Istituto, nel Patto di Corresponsabilità.

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 team preposto , si confronterà annualmente per effettuare modifiche al documento laddove ce ne fosse bisogno.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

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

Azioni da svolgere nei prossimi 3 anni:

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

Capitolo 2 - Formazione e 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.

E' necessario, sviluppare un curricolo verticale che possa sviluppare una cittadinanza sempre più
consapevole, inclusiva ,responsabile e partecipe, e che sviluppi le competenze digitali.

PROFILO DELLE COMPETENZE DIGITALI AL TERMINE DEL PRIMO CICLO DI ISTRUZIONE
Le "Indicazioni per il Curricolo per la Scuola dell'Infanzia e per il primo ciclo di istruzione", emanate con
D.M. n.254 del 16/11/2012 gazzetta ufficiale n.30 del 05/02/2013, individuano i traguardi per lo sviluppo delle competenze digitali al termine del primo ciclo: L'alunno [...] "ha buone competenze digitali, usa con consapevolezza le tecnologie della comunicazione per ricercare e analizzare dati ed informazioni, per distinguere

informazioni attendibili da quelle che necessitano di approfondimento, di controllo e di verifica e per interagire con soggetti diversi nel mondo. Utilizza la lingua inglese nell'uso delle tecnologie dell'informazione e della comunicazione".
Questi traguardi si declinano nelle seguenti Abilità – Conoscenze e Competenze:

CURRICOLI DEL PRIMO CICLO DI ISTRUZIONE - SCUOLA INFANZIA - PRIMARIA E SECONDARIA DI I GRADO –

COMPETENZE DIGITALI
Competenze finali:

- Padroneggiare le abilità e le tecniche di utilizzo delle nuove tecnologie.
- Utilizzare le nuove tecnologie con autonomia e responsabilità nel rispetto degli altri, prevenendo ed evitando i pericoli

SCUOLA DELL'INFANZIA
TRAGUARDI ATTESI IN USCITA ABILITÀ CONOSCENZE
Utilizzare le nuove tecnologie per giocare, svolgere compiti, acquisire informazioni, con la supervisione dell'insegnante.
Muovere correttamente il mouse e i suoi tasti.
Utilizzare i tasti delle frecce direzionali, dello spazio, dell'invio
Individuare e aprire icone relative a comandi, file, cartelle
Individuare e utilizzare, su istruzioni dell'insegnante, il comando "salva" per un documento già predisposto e nominato dal docente stesso.
Eseguire giochi ed esercizi di tipo logico, linguistico, matematico, topologico, al computer. Prendere visione di lettere e forme di scrittura attraverso il computer.
Prendere visione di numeri e realizzare numerazioni utilizzando il computer.
SCUOLA PRIMARIA
TRAGUARDI ATTESI IN USCITA ABILITÀ CONOSCENZE
Utilizzare con dimestichezza le più comuni tecnologie dell'informazione e della comunicazione, individuando le soluzioni potenzialmente utili ad un dato contesto applicativo, a partire dall'attività di studio.
Essere consapevole delle potenzialità, dei limiti e dei rischi dell'uso delle tecnologie dell'informazione e della comunicazione, con particolare riferimento al contesto produttivo, culturale e sociale in cui

vengono applicate.
Utilizzare strumenti informatici e di comunicazione per elaborare dati, testi e immagini e produrre documenti in diverse situazioni.
Conoscere gli elementi basilari che compongono un computer e le relazioni essenziali fra di essi.
Collegare le modalità di funzionamento dei dispositivi elettronici con le conoscenze scientifiche e tecniche acquisite.
Utilizzare materiali digitali per l'apprendimento
Utilizzare il PC, periferiche e programmi applicativi.
Utilizzare la rete per scopi di informazione, comunicazione, ricerca e svago.
Riconoscere potenzialità e rischi connessi all'uso delle tecnologie più comuni, anche informatiche.

FINE SCUOLA SECONDARIA DI I GRADO
TRAGUARDI ATTESI IN USCITA ABILITÀ CONOSCENZE
Utilizzare con dimestichezza le più comuni tecnologie dell'informazione e della comunicazione, individuando le soluzioni potenzialmente utili ad un dato contesto applicativo, a partire dall'attività di studio.
Essere consapevole delle potenzialità, dei limiti e dei rischi dell'uso delle tecnologie dell'informazione e della comunicazione, con particolare riferimento al contesto produttivo, culturale e sociale in cui vengono applicate.
Utilizzare la rete per scopi di informazione e ricerca.
Padroneggiare azioni e procedure per aprire e usare programmi e applicativi. Esplorare e selezionare i diversi programmi applicativi.
Rilevare la credibilità e l'affidabilità delle fonti comuni di dati, informazioni e contenuti digitali
Riconoscere dove organizzarli in modo semplice in un ambiente strutturato.
Condividere dati, informazioni e contenuti digitali e per l'interazione.
Identificare adeguati mezzi di comunicazione semplici per un determinato contesto.
Utilizzare strumenti informatici per produrre testi, ipertesti, ritoccare e/o adattare immagini e creare prodotti multimediali.
Utilizzare strumenti informatici per salvare ed organizzare documenti in cartelle e sottocartelle. Usare i vari dispositivi informatici e della comunicazione in modo corretto.

- Effettuare correttamente download e upload.
- Creare, gestire e rinnovare la password personale.
- Effettuare correttamente login e logout.
- Effettuare correttamente connessione e disconnessione.
- Conoscere e rispettare le regole del copyright.

- Riconoscere potenzialità e rischi connessi all'uso delle tecnologie più comuni, anche informatiche.
- Individuare semplici problemi tecnici nell'utilizzo dei dispositivi e delle tecnologie digitali.
- Identificare semplici soluzioni per risolverli.
- Individuare esigenze, riconoscere semplici strumenti digitali e possibili risposte tecnologiche per soddisfarli.
- Scegliere semplici modalità per adattare e personalizzare gli ambienti digitali alle esigenze personali.

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

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

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

Il nostro Istituto riconosce e favorisce la partecipazione del personale ad iniziative promosse sia direttamente dalla scuola, sia quelle liberamente scelte dai docenti .
La formazione interna alla scuola è organizzata dall'Animatore digitale ,con il supporto del team digitale .

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.

E' necessaria la formazione di tutti i docenti sull'uso consapevole e sicuro di Internet e sui rischi della rete. La scuola promuove iniziative di formazione e sensibilizzazione alle tematiche mediante seminari, conferenze e dibattiti, corsi di formazione interni ed esterni e qualsiasi iniziativa promuova un uso consapevole e sicuro delle TIC**.**

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

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

I genitori, nell'azione di corresponsabilità didattico-educativa, rappresentano un punto di forza per l'implementazione dei rapporti "scuola-famiglia", quale garanzia e rispetto degli impegni, di natura anche pedagogica, sottoscritti e condivisi nello stesso Patto di corresponsabilità.

Il nostro piano d'azioni

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

Scegliere almeno 1 di queste azioni

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

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

Scegliere almeno 1 di queste azioni

- Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.
- Coinvolgere una rappresentanza dei genitori per individuare i temi di maggiore interesse nell'ambito dell'educazione alla cittadinanza digitale.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare incontri con esperti per i docenti sulle competenze digitali.

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.

- Predisposizione e condivisione con l'intera comunità scolastica di un'informativa che illustri il ruolo del DPO, la tipologia di dati raccolti, il loro utilizzo e il fine per cui vengono utilizzati;

  - All'atto dell'iscrizione è richiesto alle famiglie di firmare un'autorizzazione scritta per consentire l'uso didattico di immagini e video;

  - Predisposizione di una liberatoria specifica per la condivisione di immagini e video durante eventi a carattere pubblico particolarmente rilevanti;

  - Predisposizione di una liberatoria specifica per la condivisione di elaborati ai fini della partecipazione a concorsi, a eventi pubblici;

  - Predisposizione di liberatorie specifiche, contenenti le modalità di trattamento, la

  conservazione dei dati raccolti e le misure di sicurezza adottate, per la somministrazione di questionari di ricerca e per la partecipazione ad attività che coinvolgono personale esterno alla scuola;

  - Regolamentazione sull'uso di dispositivi in grado di registrare e di strumenti compensativi

  previsti nei PdP/PEI.

  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.

LIBERATORIA PER L'UTILIZZO E LA CONDIVISIONE DI IMMAGINI, AUDIO, VIDEO DI SOGGETTI MINORI

Io sottoscritto/a (genitore/tutore) _____

_____

Nato/a a_____ il ___/___/_____ residente

a _____ via/piazza _____,
CAP_____,
Provincia_____

domicilio (se diverso dalla residenza)

via/piazza

_____,
CAP_____,
Provincia_____

Tel. _____ e-mail _____

Codice Fiscale Nr. __

_

dichiaro di aver ricevuto completa informativa ai sensi degli art. 13 e art. 14 del Regolamento UE 2016/679 in materia di protezione dei dati personali fornitami con il presente documento e, dichiarando di essere nel pieno possesso dei diritti di esercizio della responsabilità genitoriale/tutoria nei confronti del minore:

☐ esprimo il consenso ☐ non esprimo il consenso

Affinché il Titolare del Trattamento riprenda il minore in registrazioni video, audio e foto da solo, con i compagni, con insegnanti e operatori scolastici, durante lo svolgimento di attività educative didattiche e progettuali organizzate dall'IC "Don Milani Uno-Maiorano" e che tali registrazioni video, audio, immagini siano condivise:

- all'interno di tutti i materiali promozionali e/o canali di comunicazione del Titolare del Trattamento (incluso il sito internet ed i canali social) e/o individuati dal Titolare del Trattamento per le sue campagne pubblicitarie e di comunicazione.

• _ _ _

Io sottoscritto/a (genitore/tutore) _____
_____

Nato/a a_____ il ___/___/_____ residente a _____ via/piazza _____, CAP_____, Provincia_____

domicilio (se diverso dalla residenza)

via/piazza _____, CAP_____, Provincia_____

Tel. _____ e-mail _____

Codice Fiscale Nr. __ _

dichiaro di aver ricevuto completa informativa ai sensi degli art. 13 e art. 14 del Regolamento UE 2016/679 in materia di protezione dei dati personali fornitami con il presente documento e, dichiarando di essere nel pieno possesso dei diritti di esercizio della responsabilità genitoriale/tutoria nei confronti del minore:

□ esprimo il consenso □ non esprimo il consenso

Affinché il Titolare del Trattamento riprenda il minore in registrazioni video, audio e foto da solo, con i compagni, con insegnanti e operatori scolastici, durante lo svolgimento di attività educative didattiche e progettuali organizzate dall'IC "Don Milani Uno-Maiorano" e che tali registrazioni video, audio, immagini siano condivise:

- all'interno di tutti i materiali promozionali e/o canali di comunicazione del Titolare del Trattamento (incluso il sito internet ed i canali social) e/o individuati dal Titolare del Trattamento per le sue campagne pubblicitarie e di comunicazione.

- **GENITORI/TUTORI LEGALI**

del minore _____ _____

Nato/a a_____ il ___/___/_____ residente a _____ via/piazza _____, CAP_____, Provincia_____

domicilio (se diverso dalla residenza)

via/piazza _____, CAP_____, Provincia_____

Tel. _____ e-mail _____

Codice Fiscale Nr.

La presente liberatoria è valida per l'intero ciclo scolastico. Ogni diversa volontà o revoca della presente liberatoria non potrà che avvenire con la forma scritta.

Il consenso all'utilizzo dei dati personali, compresi immagini, audio e video, riferiti al minore potrà essere revocato dai genitori/tutori in qualsiasi momento con comunicazione scritta (tramite e-mail, posta ordinaria) agli indirizzi reperibili dell'Istituto con effetti futuri alla data di richiesta, facendo salvi gli usi già posti in essere in base alla presente liberatoria.

L'utilizzo dei dati sarà considerato a titolo gratuito, anche ai sensi dell'articolo 10, cod. civ., e degli articoli 96 e 97, Legge 22 Aprile 1941 n. 633 in materia di Protezione del diritto d'autore e di altri diritti connessi al suo esercizio.

L'autorizzazione dei genitori/tutori rispetto al trattamento dei dati personali del soggetto minore di cui sopra è prestata ai sensi dell'art. 2-quinquies del Decreto Legislativo 196/2003.

_____ ___/___/_____

_____

Nome per esteso del genitore/tutore legale

Data Firma

_____ ___/___/_____

_____

Nome per esteso del genitore/tutore legale Data Firma

(In caso di esercizio congiunto della responsabilità genitoriale, sarà necessario il consenso di entrambi i genitori).

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.

Gli studenti si impegnano a:
utilizzare in modo consapevole e corretto la RETE e i dispositivi telematici, nel rispetto della privacy e della dignità propria e altrui;
rispettare le consegne dei docenti;
non scaricare materiali e software senza autorizzazione;
non utilizzare unità removibili personali senza autorizzazione;
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.

3.3 - Strumenti di comunicazione online

Le tecnologie digitali sono in grado di ridefinire gli ambienti di apprendimento, supportando la comunicazione a scuola e facilitando un approccio sempre più collaborativo. L'uso degli strumenti di comunicazione online a scuola, al fianco di quelli più tradizionali, ha l'obiettivo di rendere lo scambio comunicativo maggiormente interattivo e orizzontale. Tale uso segue obiettivi e regole precise correlati alle caratteristiche, funzionalità e potenzialità delle tecnologie digitali.

La nostra DS coordina la comunicazione interna ed esterna del nostro Istituto a partire da un piano di comunicazione in grado di trasmettere all'esterno l'identità, i valori, le azioni, i progetti e l'idea di educazione che la scuola porta avanti. Sono stati individuati alcuni docenti responsabili del Sito Web e della pagina FB di Istituto. Altri mezzi di comunicazione online in dotazione alla scuola sono: il registro elettronico con tutte le sue funzionalità, lo sportello di segreteria digitale, la mail, strumenti di messaggistica istantanea come whatsapp (docenti-genitori esclusivamente per fini didattici), ulteriori applicativi e piattaforme di lavoro condiviso e collaborativo come G Suite for

Education, app incluse.

Il registro elettronico consente una comunicazione chiara e immediata con le famiglie relativamente a:

1. andamento scolastico (assenze, argomenti lezioni e compiti, note disciplinari);

2. risultati scolastici (documenti di valutazione);

3. udienze (prenotazioni colloqui individuali);

4. eventi (agenda eventi);

5. comunicazione varie (comunicazioni di classe, comunicazioni personali).

Tutte le comunicazioni scuola-famiglia contenenti dati sensibili sono visibili da parte della famiglia dell'alunno interessato e non dal resto della classe. Solo il DS e i docenti del CDC possono avere accesso a tali informazioni.

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 dispone il divieto dell'utilizzo del cellulare o di altri dispositivi elettronici per uso personale. La violazione di tale divieto

configura un'infrazione disciplinare rispetto alla quale la scuola è tenuta ad applicare apposite sanzioni.

Sia alunni (quando autorizzati dal docente) e i docenti sono tenuti a spegnere i propri cellulari prima dell'ingresso in aula.

Il nostro piano d'azioni

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

Scegliere almeno 1 di queste azioni:

- Organizzare uno o più eventi o attività volti a consultare i docenti dell'Istituto perredigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola
- Organizzare incontri per la consultazione degli studenti/studentesse suindicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola
- Organizzare incontri per la consultazione dei genitori su indicazioni/regolamentisull'uso dei dispositivi digitali personali a scuola
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

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

Scegliere almeno 1 di queste azioni:

- Organizzare uno o più eventi o attività volti a consultare i docenti dell'Istituto perredigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali.
- Organizzare incontri per la consultazione degli studenti/studentesse suindicazioni/regolamenti sull'uso dei dispositivi digitali personali
- Organizzare incontri per la consultazione dei genitori su indicazioni/regolamentisull'uso dei dispositivi digitali personali

- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

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

4.1 - Sensibilizzazione e Prevenzione

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

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

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

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

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

Allo scopo di sensibilizzare e prevenire il fenomeno del cyberbullismo il nostro istituto ha previsto incontri con le forze dell'ordine, con i Carabinieri, con la Polizia Postale con la Guardia di Finanza.
Verranno integrati i Regolamenti di Istituto e il Patto di Corresponsabilità con specifici riferimenti a condotte di cyberbullismo e

relative sanzioni disciplinari commisurate alla gravità degli atti compiuti;
Ogni Consiglio di Classe provvederà a dedicare alcuni momenti al fenomeno, con letture di brani specifici, proiezione di video e lezioni specifiche.

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 nostro istituto , già da tempo ha avviato procedure e attività mirate alla prevenzione al contrasto del cyberbullismo quali: la partecipazione al Progetto "MaBasta bullismo in Puglia" ,organizzazione di convegni e conferenze con la presenza delle Forze dell'ordine, affissione nelle aule il Manifesto **Parole_O_Stili** e intende nel tempo proseguire su questa strada, attivando altri e diversi percorsi di prevenzione.

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.

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere in relazione a questa problematica.

Affissione nelle aule il Manifesto delle **Parole_O_Stili**

Nelle ore di educazione civica si forniranno 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

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?

Verranno forniti al personale della scuola, agli studenti e alle loro famiglie strumenti finalizzati al riconoscimento e alla prevenzione del fenomeno.

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 Legge 19 luglio 2019 n. 69, all’articolo 10, ha introdotto in Italia il reato di "revenge porn", ossia

la diffusione illecita di immagini o di video sessualmente espliciti.

I rischi del sexting, legati al revenge porn, possono contemplare: violenza psico-sessuale,

umiliazione, bullismo, cyberbullismo, molestie, stress emotivo che si riversa anche sul corpo insieme a ansia diffusa, sfiducia nell’altro 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.

Il nostro Istituto si prefigge di fornire al personale della scuola, agli studenti e alle loro famiglie strumenti finalizzati al riconoscimento e alla prevenzione del fenomeno.

Si progetteranno per gli studenti percorsi guidati su educazione all'affettivà e alla

sessualità, anche attraverso il ricorso a psicologi specializzati.

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.

Su tale problematica verrà realizzata dal nostro istituto, un'attività di sensibilizzazione al fenomeno promuovendo i servizi di Generazioni Connesse.

Il nostro piano d'azioni

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

Scegliere almeno 1 di queste azioni:

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

Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti agli/lle studenti/studentesse, con il coinvolgimento di esperti.

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

Scegliere almeno 1 di queste azioni:

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

Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti agli/lle studenti/studentesse, con il coinvolgimento di esperti.

Promuovere incontri e laboratori per studenti e studentesse dedicati all' Educazione Civica Digitale.

Organizzare uno o più incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/lle studenti/studentesse.

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.

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

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.

E' presente nella scuola la Bully box destinata ad accogliere i messaggi che gli alunni, in forma anonima, vorranno segnalare per denunciare episodi e/o situazioni presenti. I messaggi verranno ritirati, con cadenza quindicinale, dalla referente d'istituto, prof.ssa Marina Scircoli. Nella suddetta cassetta potranno essere inseriti anche racconti di esperienze positive e proposte concrete.

Moduli di segnalazione

MODULO SEGNALAZIONE BULLISMO/CYBERBULLISMO/COMPORTAMENTI AGGRESSIVI

Usa questo modulo per segnalare comportamenti offensivi, aggressioni fisiche, prese in giro, isolamento dal gruppo che si sono verificati tra gli alunni a scuola, nel tragitto tra casa e scuola e viceversa, sui social network o tramite messaggi e giochi online.

Nella segnalazione puoi non riportare il tuo nome e cognome ma è consigliato dare tutte le informazioni possibili perché la Scuola possa intervenire. Puoi anche segnalare verbalmente ad un insegnante, ai docenti del Team Antibullismo o al personale scolastico.

Nome e cognome di chi fa la segnalazione (facoltativo):_____

Oggi è (indicare giorno/mese/anno):_____

Io sono (indicane uno):

L'alunno che ha subito (indica il nome, facoltativo) _____

Un amico/a della vittima (indica il nome, facoltativo) _____

Un testimone (indica il nome, facoltativo) _____

Un genitore, nome_____

Un insegnante, nome_____

Altro:_____

Chi è l'aggressore _____ e quale classe frequenta_____

Chi è l'aggressore _____ e quale classe frequenta_____

Erano presenti altre persone? Sì No

Se sì, riporta i loro nomi:_____
____

_____
_____ e indica quale classe frequentano_____

Descrivi brevemente il problema dando esempi concreti di quello che è successo, quando e dove

_____
_____
_____
_____

RISERVATO ALLA COMPILAZIONE DEL DOCENTE, DEL REFERENTE BULLISMO E CYBERBULLISMO DELLA SCUOLA O DEI DOCENTI DEL TEAM ANTIBULLISMO CHE RICEVONO LA SEGNALAZIONE

La segnalazione è avvenuta:

A voce Tramite modulo reperibile attraverso la Referente bullismo e cyberbullismo

Ricevuta da: _____ Data Ricezione: _____

Modulo di segnalazione dei casi di presunto bullismo e/o di cyber bullismo

Nome di chi compila la segnalazione…….
Data……..

1. La persona che ha segnalato il caso di presunto bullismo/cyberbullismo è

☐ La vittima……

☐ Un compagno della vittima, nome……

☐ Madre/padre/tutore della vittima

nome……..

☐ Insegnante
nome……

☐
Altri……
…

2.
Vittima……
…

Altre
vittime……

3. Bullo o bulli (o presunti)

Nome……
……..

Nome……
……..

Nome……
……..

4. Descrizione del problema presentato, dando esempi concreti degli episodi di prepotenza
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……

5. Quante volte si sono verificati gli episodi?
……
……
……
……

.....

5.3. - Gli attori sul territorio

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

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

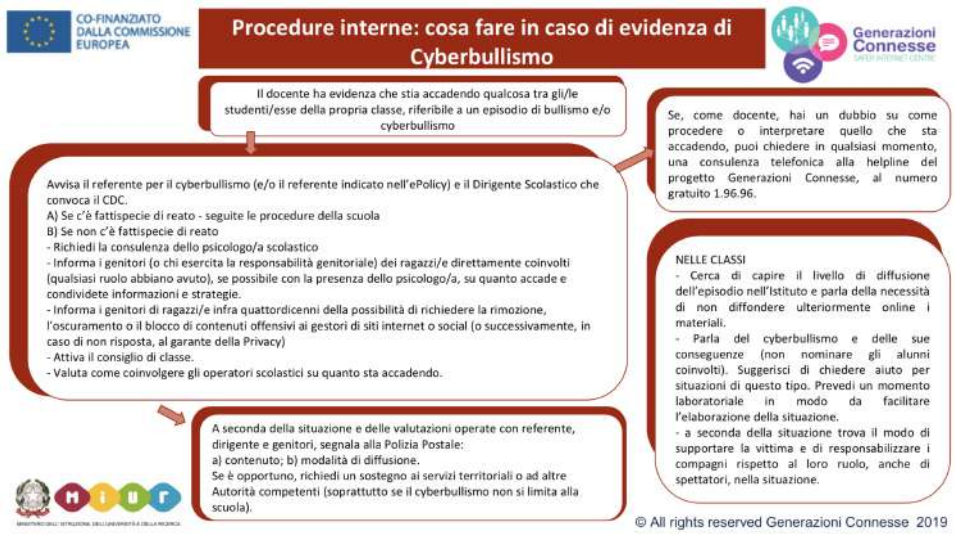
A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all'utilizzo di Internet può presentare.

- **Comitato Regionale Unicef**: laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni)**: svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare attenzione alla tutela dei minori.
- **Ufficio Scolastico Regionale**: supporta le scuole in attività di prevenzione ed anche nella segnalazione di comportamenti a rischio correlati all'uso di Internet.
- **Polizia Postale e delle Comunicazioni**: accoglie tutte le segnalazioni relative a comportamenti a rischio nell'utilizzo della Rete e che includono gli estremi del reato.
- **Aziende Sanitarie Locali**: forniscono supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in Rete. In alcune regioni, come il Lazio e la Lombardia, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da Internet e alle situazioni di rischio correlate.
- **Garante Regionale per l'Infanzia e l'Adolescenza e Difensore Civico**: segnalano all'Autorità Giudiziaria e ai Servizi Sociali competenti; accolgono le segnalazioni di presunti abusi e forniscono informazioni sulle modalità di tutela e di esercizio dei diritti dei minori vittime. Segnalano alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.

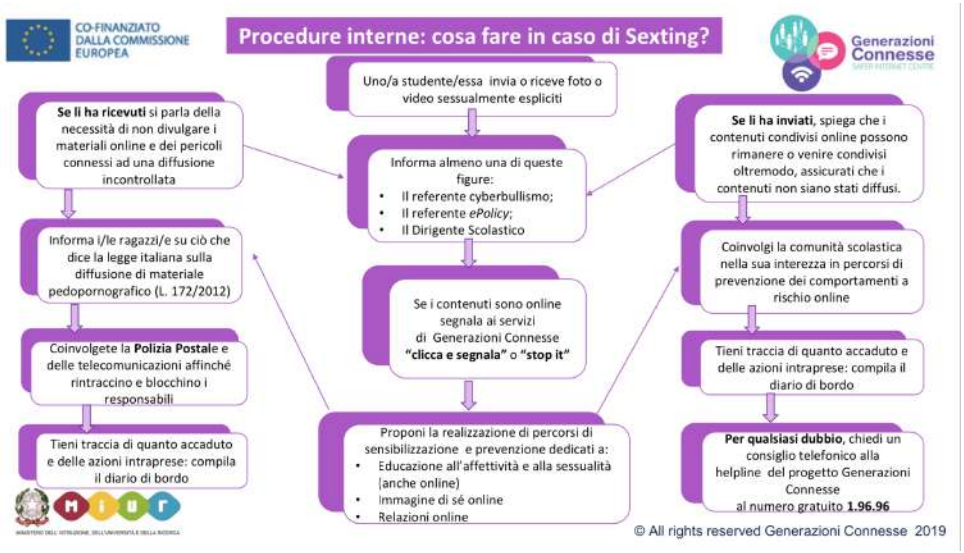
- **Tribunale per i Minorenni**: segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

5.4. - Allegati con le procedure

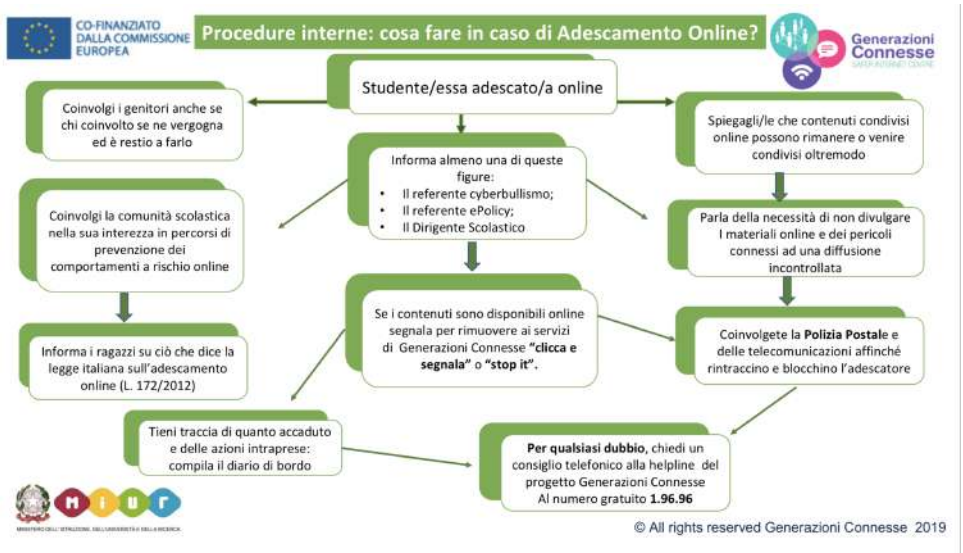
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



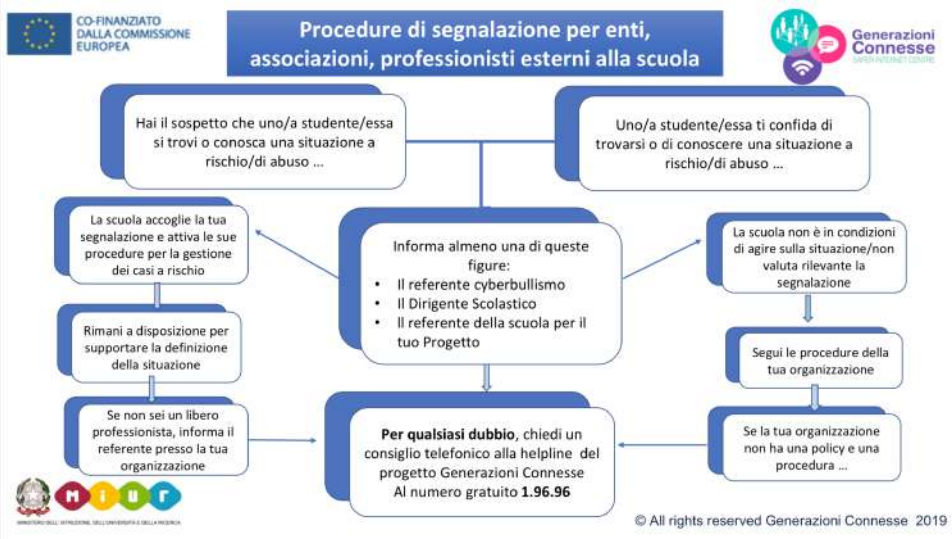
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



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



Altri allegati

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

Il nostro piano d'azioni

Non è prevista nessuna azione.