Documento di ePolicy

APIC824008

MONTEGRANARO ISC

VIA MARTIRI D'UNGHERIA 98 - 63812 - MONTEGRANARO - FERMO (AP)

Chiara Cudini

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.

Dall'esistenza di questo bisogno di promozione di un uso sicuro e positivo delle tecnologie scaturisce il presente documento, prodotto dalla scuola nell'ambito del progetto "Generazioni connesse",

promosso dal MIUR per offrire alle istituzioni scolastiche interessate un supporto effettivo nella definizione di misure di prevenzione, rilevazione e gestione delle problematiche derivanti da un uso non consapevole delle tecnologie digitali tra gli studenti, anche attraverso la formazione degli insegnanti e la sensibilizzazione dei genitori.

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.

1. **IL DIRIGENTE SCOLASTICO** è garante della sicurezza di tutti i membri della comunità scolastica. Si forma adeguatamente sulla sicurezza e sulla prevenzione di problematiche online e offline, promuove la cultura della sicurezza online e dà il proprio contributo all'organizzazione di corsi di formazione specifici per tutte le figure scolastiche sull'utilizzo positivo e responsabile delle TIC.
2. **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, ed è inoltre uno dei promotori di percorsi di formazione interna all'istituto negli ambiti di sviluppo della scuola digitale.
3. **IL REFERENTE BULLISMO E CYBERBULLISMO** coordina e promuove iniziative specifiche per la prevenzione e il contrasto dei suddetti fenomeni, si avvale della collaborazione delle Forze di polizia e coinvolge, con progetti e percorsi formativi ad hoc, studenti, colleghi e genitori.
4. **I DOCENTI** diffondono la cultura dell'uso responsabile delle TIC e della Rete, integrano parti del curriculum della propria disciplina con approfondimenti ad hoc, usano tecnologie digitali nella loro didattica, segnalano al Dirigente Scolastico qualunque problematica, violazione o abuso, anche online, che vede coinvolti studenti e studentesse.
5. **IL PERSONALE ATA** nel rispetto delle proprie funzioni di natura amministrativa, contabile, gestionale e di sorveglianza, è tenuto a utilizzare con il massimo rispetto gli strumenti presenti nella scuola, seguendo i regolamenti vigenti e minimizzando gli sprechi delle risorse a disposizione. Inoltre, è coinvolto nella segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo.
6. **GLI STUDENTI** sono chiamati a utilizzare al meglio le tecnologie digitali in coerenza con quanto richiesto dai docenti, si tutelano e tutelano i propri compagni, partecipano attivamente a progetti ed attività che riguardano l'uso positivo delle TIC.
7. **I GENITORI**, in continuità con l'istituto scolastico, educano i propri figli ad un uso consapevole delle TIC, della Rete e dei propri device, accettano e condividono quanto scritto nella ePolicy d'istituto e comunicano ai docenti i problemi rilevati quando i propri figli non usano responsabilmente le tecnologie digitali o Internet.

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).

I soggetti esterni che entrano in relazione con la scuola si conformano alla politica della stessa riguardo l'uso consapevole della Rete e delle TIC, promuovono comportamenti sicuri ed assicurano la protezione degli studenti durante le attività che si svolgono insieme.

Nello specifico, i soggetti esterni dovranno:

- leggere, comprendere e aderire a questa ePolicy;
- aver cura degli strumenti in dotazione;
- non divulgare agli alunni le credenziali di accesso alla rete WIFI;
- installare e utilizzare solo software autorizzati;
- lasciare invariate le impostazioni dei dispositivi della scuola;
- segnalare celermente eventuali malfunzionamenti;
- non salvare sui dispositivi utilizzati file contenenti dati personali e/o sensibili;
- non memorizzare credenziali, indirizzi email e file personali sui dispositivi;
- controllare l'uso corretto della strumentazione da parte degli alunni, informandoli sul corretto uso della Rete;
- assicurarsi di aver effettuato il logout da ogni servizio prima di lasciare la postazione;
- accertarsi che tutti i pc e gli altri strumenti siano stati spenti nel modo corretto;
- segnalare eventuali episodi di bullismo/cyberbullismo.

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.

Ciò garantirà una completa condivisione da parte dell'intera comunità scolastica e potrà rendere il presente documento una base di partenza per azioni e iniziative, quali una discussione aperta sui contenuti e sulle pratiche indicate, sulle modalità per inserire le tematiche di interesse della ePolicy nel curricolo, nonchè un confronto in merito alla necessità di apportarvi modifiche e miglioramenti.

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.

I provvedimenti disciplinari nei confronti dell'alunno che ha commesso un'infrazione alla ePolicy dovranno essere proporzionati all'età dello studente e alla gravità dell'infrazione commessa e potranno essere così graduati:

- richiamo verbale;
- sanzioni commisurate alla gravità della violazione commessa;
- nota sul diario trascritta nel registro elettronico al fine di informare i genitori;
- convocazione dei genitori per un colloquio con l'insegnante interessato;
- convcazione dei genitori per un colloquio con il Dirigente Scolastico.

Qualora tali infrazioni dovessero configurarsi come reato, ne sarà data tempestiva segnalazione al Dirigente Scolastico per gli adempimenti del caso.

Per ogni infrazione alle regole stabilite, gli studenti riceveranno tutti gli strumenti per affrontare le conseguenze dei loro errori ed essere rieducati in merito con azioni mirate a responsabilizzarli e a cambiare il loro atteggiamento.

Verranno inoltre messe preventivamente in atto, in special modo in occasione del Safer Internet Day, attività laboratoriali miranti a sviluppare negli alunni una sempre maggiore consapevolezza dei rischi legati ad un uso imprudente ed improprio delle TIC e della Rete.

1.6 - Integrazione dell'ePolicy con Regolamenti esistenti

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

Anche il PTOF verrà integrato con riferimenti al presente documento.

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 per l'implementazione della ePolicy potrà avvenire al termine dell'anno scolastico, contestualmente al Rapporto di Autovalutazione e sulla base dei casi problematici riscontrati e della loro gestione, oppure all'inizio dell'anno scolastico, in fase di revisione del PTOF, a cura del Dirigente Scolastico, dell'Animatore digitale, del Referente bullismo/cyberbullismo e del Gruppo di Lavoro ePolicy, anche attraverso la somministrazione ad alunni e docenti di questionari atti a verificare l'insorgenza di nuove necessità e la revisione di tecnologie esistenti.

Il nostro piano d'azioni

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

- Creazione del gruppo di lavoro ePolicy;
- Realizzazione di un sistema di monitoraggio delle attività;
- Realizzazione di un'assemblea per discutere delle attività di progetto.

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

- Implementare la dotazione di strumenti informatici (LIM/proiettori + pc + casse) in tutte le aule della scuola primaria e secondaria;
- Utilizzare regolarmente il registro elettronico nella scuola primaria e secondaria;
- Allestire un laboratorio di informatica nella scuola secondaria.

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.

TRAGUARDI AL TERMINE DELLA SCUOLA DELL'INFANZIA

Competenze

- Sviluppare ed utilizzare il pensiero computazionale
- Acquisire informazioni delle competenze specifiche
- Utilizzare le nuove tecnologie per giocare
- Svolgere semplici attività tra cui quelle di coding con la supervisione dell'insegnante

Abilità

- Muovere correttamente il mouse e i suoi tasti
- Utilizzare i tasti delle frecce direzionali
- Aprire e chiudere un programma
- 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

- Visionare immagini, opere artistiche, filmati

Conoscenze

- Il computer ed alcuni suoi usi
- Mouse
- Tastiera
- Icone principali di Windows e Microsoft Word

TRAGUARDI AL TERMINE DELLA SCUOLA PRIMARIA

Competenze

- Utilizzare le più comuni tecnologie dell'informazione e della comunicazione in contesto di studio
- Conoscere potenzialità, limiti e rischi dell'uso delle tecnologie

Abilità

- 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 essi
- Utilizzare materiali digitali per l'apprendimento
- Utilizzare la rete per scopi di informazione, ricerca e svago
- Riconoscere potenzialità e rischi connessi all'uso delle tecnologie più comuni, anche informatiche

Conoscenze

- Il sistema operativo e i più comuni software applicativi
- Procedure per la produzione di testi e presentazioni
- I motori di ricerca
- Caratteristiche e potenzialità tecnologiche degli strumenti di uso comune

TRAGUARDI AL TERMINE DELLA SCUOLA SECONDARIA DI PRIMO GRADO

Competenze

- Utilizzare con dimestichezza le più comuni tecnologie dell'informazione e della comunicazione in contesti di studio
- Essere consapevole delle potenzialità, dei limiti e dei rischi dell'uso delle tecnologie dell'informazione e della comunicazione

Abilità

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

Conoscenze

- Le applicazioni tecnologiche quotidiane e le relative modalità di funzionamento
- I dispositivi informatici di input e output
- Il sistema operativo e i più comuni software applicativi
- Procedure per la produzione di mappe, testi, ipertesti, presentazioni ed utilizzo dei fogli di calcolo
- Procedure di utilizzo di reti informatiche per ottenere dati e fare ricerche
- Caratteristiche e potenzialità tecnologiche degli strumenti tecnologici di uso comune
- Utilizzo sicuro e legale di reti informatiche per ottenere dati e comunicare

---

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

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

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

La formazione dei docenti in merito all'utilizzo e all'integrazione delle TIC nella didattica potrà avvenire a livello interno ed esterno.

Della formazione interna si occupa prevalentemente l'Animatore digitale unitamente ai docenti del team dell'innovazione. La suddetta formazione è improntata alla condivisione di esperienze significative e buone pratiche.

Per quanto riguarda invece la formazione esterna, la scuola assicura tempestiva e capillare informazione su corsi, convegni e seminari inerenti le tecnologie dell'informazione e della comunicazione impiegate nella didattica.

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'anno scolastico in corso (2019/2020) il nostro istituto aderisce a due progetti presentati da enti ed associazioni in merito all'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.

La scuola primaria è coinvolta nel progetto *STOP BULLYNG 2.0: peer education e digital storytelling per contrastare bullismo e cyberbullismo*.

Il progetto articola in due fasi la formazione rivolta ai docenti: dapprima si è tenuto un incontro informativo/formativo tra insegnanti, famiglie e figure professionali coinvolte; a questo ha fatto seguito un incontro tra la psicologa e la sociologa dell'Associazione Sipea con gli insegnanti coinvolti nel progetto per discutere dell'uso degli strumenti di comunicazione reperibili in Rete da parte dei bambini e per progettare le varie fasi di lavoro per la realizzazione di storytelling.

La scuola secondaria di primo grado è coinvolta nel progetto *I CAMPIONI DEL VILLAGGIO DIGITALE*.

Per questo progetto è prevista una fase di formazione per i docenti tramite un incontro con appartenenti all'Associazione RED e due Commissari della Polizia Postale e un'altra fase di specifiche attività didattiche per gli alunni.

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

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

La scuola ha avviato già dall'anno scolastico 2018/2019 attività per sensibilizzare ed informare in vari modi le famiglie rispetto all'importanza di un corretto uso delle tecnologie da parte dei ragazzi, a casa ed a scuola.

Nell'anno scolastico in corso sono programmati due incontri rivolti ai genitori per conseguire i seguenti obiettivi:

- sensibilizzare sui temi del bullismo e del cyberbullismo ed offrire un primo momento di ascolto;
- fornire informazioni sui fenomeni del bullismo e del cyberbullismo;
- conoscere le implicazioni socio-emotive coinvolte nei processi della relazione reale e virtuale.

Proprio nell'ottica del coinvolgimento di tutte le parti attive del processo educativo, gli alunni della scuola primaria produrranno una storytelling, mentre gli alunni della scuola secondaria di primo grado concluderanno il loro progetto attraverso una giornata con genitori, esperti e docenti effettuando una sfida finale sui temi trattati in un "Villaggio digitale".

Il nostro piano d'azioni

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

- Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo

consapevole e sicuro di Internet e delle tecnologie digitali.

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

- 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.
- Organizzare incontri con esperti per i docenti sulle competenze digitali.
- Organizzare incontri con esperti per i genitori sull’educazione alla cittadinanza digitale.

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

3.1 - Protezione dei dati personali

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

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

Ogni giorno a scuola vengono trattati numerosi dati personali sugli studenti e sulle loro famiglie. Talvolta, tali dati possono riguardare informazioni sensibili, come problemi sanitari o particolari disagi sociali. Il "corretto trattamento dei dati personali" a scuola è condizione necessaria per il rispetto della dignità delle persone, della loro identità e del loro diritto alla riservatezza. Per questo è importante che le istituzioni scolastiche, durante lo svolgimento dei loro compiti, rispettino la privacy, tutelando i dati personali dei soggetti coinvolti, in particolar modo quando questi sono minorenni.

La protezione dei dati personali è un diritto fondamentale dell'individuo ai sensi della Carta dei diritti fondamentali dell'Unione europea (art. 8), tutelato dal Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 (relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati).

Anche le scuole, quindi, hanno oggi l'obbligo di adeguarsi al cosiddetto GDPR (General Data Protection Regulation) e al D.Lgs. 10 agosto 2018, n. 101, entrato in vigore lo scorso 19 settembre.

In questo paragrafo dell'ePolicy affrontiamo tale problematica, con particolare riferimento all'uso delle tecnologie digitali, e indichiamo le misure che la scuola intende attuare per garantire la tutela della privacy e il diritto alla riservatezza di tutti i soggetti coinvolti nel processo educativo, con particolare attenzione ai minori. A tal fine, l'Istituto allega alla presente ePolicy i modelli di liberatoria da utilizzare e conformi alla normativa vigente, in materia di protezione dei dati

personali.

La scuola tratta solamente i dati personali necessari al perseguimento di specifiche finalità istituzionali. Tramite apposita informativa distribuita all'inizio dell'anno scolastico, gli interessati vengono messi al corrente delle caratteristiche e delle modalità del trattamento dei loro dati.

Nelle circolari e nelle comunicazioni scolastiche non rivolte a specifici destinatari non vengono inseriti dati personali che rendono identificabili alunni coinvolti in vicende particolarmente delicate.

Le programmazioni recanti la divisione delle classi in fasce di livello ed i documenti personalizzati per singoli alunni (H, DSA, BES) vengono condivisi tra insegnanti esclusivamente in apposita area del registro elettronico.

Sono permesse a titolo gratuito le riprese video e fotografiche di visite guidate o viaggi di istruzione, cerimonie, eventi e rappresentazioni scolastiche, se destinate a un ambito personale e familiare. In caso di pubblicazione di foto e video nel sito della scuola, nella piattaforma eTwinning o nei canali social dell'istituto scolastico (pagina Facebook e canale Youtube), la scuola richiede l'esplicito consenso ai genitori degli studenti coinvolti attraverso una specifica liberatoria conforme alla normativa vigente.

La scuola rispetta le indicazioni contenute nel vademecum *La scuola a prova di privacy*, a cura del Garante per la protezione dei dati personali del 2016, oltre che i riferimenti normativi sopra citati.

3.2 - Accesso ad Internet

1. *L’accesso a Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale.*
2. *Ogni persona ha eguale diritto di accedere a Internet in condizioni di parità, con modalità tecnologicamente adeguate e aggiornate che rimuovano ogni ostacolo di ordine economico e sociale.*
3. *Il diritto fondamentale di accesso a Internet deve essere assicurato nei suoi presupposti sostanziali e non solo come possibilità di collegamento alla Rete.*
4. *L'accesso comprende la libertà di scelta per quanto riguarda dispositivi, sistemi operativi e applicazioni anche distribuite.*
5. *Le Istituzioni pubbliche garantiscono i necessari interventi per il superamento di ogni forma di divario digitale tra cui quelli determinati dal genere, dalle condizioni economiche oltre che da situazioni di vulnerabilità personale e disabilità.*

Così recita l’art. 2 della Dichiarazione dei diritti di Internet, elaborata dalla Commissione per i diritti e i doveri in Internet, commissione costituita il 27 ottobre 2014 presso la Camera dei Deputati dalla presidente Laura Boldrini e presieduta da Stefano Rodotà. Inoltre, il 30 aprile 2016 era entrato in vigore il Regolamento UE del Parlamento Europeo e del Consiglio del 25 novembre 2015, che

stabilisce le “misure riguardanti l’accesso a un’Internet aperto e che modifica la direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica e il regolamento (UE) n. 531/2012 relativo al roaming sulle reti pubbliche di comunicazioni mobili all’interno dell’Unione”.

Il diritto di accesso a Internet è dunque presente nell’ordinamento italiano ed europeo e la scuola dovrebbe essere il luogo dove tale diritto è garantito, anche per quegli studenti che non dispongono della Rete a casa. In modo coerente il PNSD (Piano Nazionale Scuola Digitale) ha tra gli obiettivi quello di “fornire a tutte le scuole le condizioni per l’accesso alla società dell’informazione e fare in modo che il “diritto a Internet” diventi una realtà, a partire dalla scuola”.

Questo perché le tecnologie da un lato contribuiscono a creare un ambiente che può rendere la scuola aperta, flessibile e inclusiva, dall’altro le consentono di adeguarsi ai cambiamenti della società e del mercato del lavoro, puntando a sviluppare una cultura digitale diffusa che deve iniziare proprio a scuola.

L'Animatore digitale, il team per l'innovazione ed il tecnico informatico si stanno adoperando per i seguenti obiettivi:

- dotare tutte le classi della scuola primaria e della scuola secondaria di primo grado di LIM o di proiettori, pc portatili e casse audio;
- potenziare la rete wireless;
- utilizzare sempre il protocollo di trasmissione dei dati https;
- aggiornare costantemente software e sistemi operativi;
- predisporre la disconnessione automatica dei dispositivi, dopo un certo tempo di inutilizzo;
- impostare i browser per l'eliminazione dei cookies alla chiusura della sessione.

Ogni pc dell'istituto è dotato di password, nota soltanto ai docenti. L'uso del pc di classe o del laboratorio informatico da parte degli alunni è permesso soltanto su autorizzazione dell'insegnante.

Una volta conseguito l'accesso ad Internet, spetta agli alunni:

- utilizzare la Rete nel modo corretto;
- rispettare le consegne dei docenti;
- non scaricare materiali e software senza autorizzazione;
- non utilizzare unità di memoria rimovibili personali senza autorizzazione;
- lasciare immutata la configurazione di sistema dei dispositivi;
- segnalare immediatamente materiali inadeguati ai propri insegnanti;
- chiudere correttamente la propria sessione di lavoro.

I docenti, invece, sono chiamati a:

- utilizzare la Rete nel modo corretto;
- non utilizzare device personali se non per uso didattico;
- formare gli studenti all'uso corretto della Rete;
- monitorare l'uso che gli studenti fanno delle tecnologie a scuola;
- compilare debitamente il registro elettronico, accedendovi attraverso una password

personale forte, periodicamente modificata, che non può essere comunicata a terzi nè agli alunni.

In questa sede è opportuno esplicitare che la scuola si farà carico di tutte le precauzioni necessarie per garantire agli studenti l'accesso a materiale appropriato, ma allo stesso tempo non può essere responsabile per l'accesso autonomo da parte degli alunni a materiali inadeguati e potenzialmente dannosi trovati online.

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.

STRUMENTI DI COMUNICAZIONE ESTERNA

(utili per fornire informazioni di servizio rivolte a studenti e genitori e per pubblicizzare e valorizzare le attività effettuate dalla comunità scolastica)

1. Pagina Facebook *IC Montegranaro*
2. Canale Youtube *IC Montegranaro*
3. Sito istituzionale https://icmontegranaro.edu.it/
4. Registro elettronico *Nuvola*, in uso presso la scuola primaria e la scuola secondaria di primo grado, attraverso il quale i genitori, previo accesso tramite password, possono visualizzare assenze, voti e note dei propri figli nonchè gli argomenti di lezione ed i compiti assegnati da ciascun docente

STRUMENTI DI COMUNICAZIONE INTERNA

(utili per facilitare e rendere più partecipata la comunicazione a scuola)

1. Registro elettronico *Nuvola*
2. Mail istituzionale apic824008@istruzione.it
3. Mail dei singoli docenti
4. Sito istituzionale https://icmontegranaro.edu.it/

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.

Di norma, agli studenti non è consentito l'uso di smartphone, tablet e pc personali a scuola, se non espressamente richiesto dal docente, esclusivamente per scopi didattici e previo consenso informato dei genitori, senza tuttavia accedere alla Rete dell'istituto.

Non è pertanto possibile scattare foto, realizzare video e diffondere il materiale se ciò non è conforme alla documentazione dell'attività didattica e se vengono lese la riservatezza e la dignità delle persone raffigurate.

I docenti possono utilizzare in classe i dispositivi della scuola, nonchè quelli personali, per realizzare tutte le attività connesse alla funzione docente e all'agire didattico.

Il nostro piano d'azioni

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

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli studenti
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte dei docenti
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte del personale ATA
- Organizzare uno o più eventi o attività volti a formare docenti ed ATA sul tema delle tecnologie digitali, della protezione dei dati personali, dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali

AZIONI (da sviluppare nell'arco dei tre anni

scolastici successivi)

- Organizzare uno o più eventi o attività volti a consultare i docenti dell'Istituto per redigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali.
- Organizzare incontri per la consultazione degli studenti e dei genitori su indicazioni sull'uso dei dispositivi digitali personali
- Organizzare uno o più eventi o attività volti a formare gli studenti e i genitori sul tema delle tecnologie digitali, della protezione dei dati personali, dell'accesso a Internet e dell'uso sicuro delle tecnologie digitali

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 scuola prevede i seguenti interventi di **SENSIBILIZZAZIONE**:

- incoraggiare gli studenti a modificare i propri comportamenti rendendoli più funzionali;
- diffondere una certa consapevolezza rispetto all'argomento di interesse;
- facilitare il coinvolgimento di soggetti esterni (ASL e Polizia Postale) in modo da mettere insieme diverse idee per lavorare ad un obiettivo comune;
- favorire la diffusione di informazioni e servizi disponibili all'utilità collettiva.

Per quanto concerne la **PREVENZIONE**, partendo dal presupposto che oggigiorno tutti gli studenti sono potenzialmente a rischio, il nostro istituto attua interventi diretti all'intera popolazione

scolastica. Un esempio è costituito dal *Safer Internet Day*, giornata annuale in cui si rifletterà sulle potenzialità e sui rischi di Internet nei tempi e nei modi più consoni per ciascun ordine di scuola. Nel caso in cui si venga a conoscenza di determinati fattori di rischio per la sicurezza presenti in uno specifico gruppo-classe, invece, verranno attuati interventi mirati e verranno previsti programmi formativi strutturati con l'obiettivo di migliorare le competenze digitali e le strategie di problem solving.

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 intende perseguire i seguenti obiettivi generali per prevenire e contrastare il Cyberbullismo:

- informare le famiglie sull'utilizzo di strumenti di parental control che limitino l'accesso a contenuti potenzialmente pericolosi in Rete;
- formare gli educatori in merito agli strumenti di comunicazione e interazione della Rete;
- far conoscere e riconoscere ai ragazzi i pericoli della Rete;
- istruire i ragazzi in merito alle strategie comportamentali per ridurre i rischi di esposizione;
- attuare percorsi di educazione alla convivenza civile e alla cittadinanza;
- predisporre momenti di formazione per i docenti sulle strategie di gestione del fenomeno.

Per affrontare il tema in classe in modo coinvolgente e partecipato, la scuola utilizzerà la mini-serie *Gaetano: storie di ordinario cyberbullismo*, realizzata da Generazioni Connesse. Gli studenti potranno visualizzare dei video nei quali ogni vicenda è strutturata mettendo in evidenza la figura del bullo e del bullizzato, e potranno scegliere soluzioni in base a come vorrebbero si concludesse la storia.

Inoltre, come già detto, il nostro istituto ha aderito a due progetti:

1. *STOPBULLYING 2.0* (scuola primaria) - peer education e digital storytelling il cui lavoro finale sarà una storytelling;
2. *I CAMPIONI DEL VILLAGGIO DIGITALE* (scuola secondaria di primo grado) - incontri con personale esperto e sfida a squadre.

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.

Nel corso dei progetti già menzionati, si inviteranno i ragazzi a riflettere sul fenomeno ed in particolare su:

- contenuti e toni delle espressioni recriminate;
- intenzioni degli autori degli insulti;
- bersagli (potenziali e non);
- contesto;
- impatto (potenziale e non).

Lo sviluppo delle competenze digitali e l'educazione ad un uso etico e responsabile delle tecnologie assumono quindi un ruolo centrale anche per la promozione della consapevolezza di queste dinamiche.

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?

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

Il nostro istituto si impegna a sensibilizzare gli studenti sulla dipendenza da Internet e dal gioco online mostrando l'utilizzo funzionale della tecnologia integrata alla didattica, in modo da rendere più consapevoli gli alunni della validità o meno delle proprie abitudini online.

Gli insegnanti, consapevoli che tecnologia e giochi formano parte integrante del mondo dei bambini e dei ragazzi, stabiliranno chiare e semplici regole di utilizzo quando vi faranno ricorso per le pratiche d'aula, ma proporranno anche delle alternative metodologiche valide.

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.

In merito ad una questione così delicata, la scuola non intende sostituirsi alla famiglia, ma collaborerà con la stessa.

Se durante lo svolgimento delle attività didattiche si dovesse incorrere nel tema (articoli di attualità, ricerca di confronto da parte degli studenti), la scuola non si sottrarrà al suo compito educante. Il suo intervento sarà soprattutto volto a far capire che:

- la condivisione di scatti intimi può essere virale ed incontrollabile;
- le fotografie possono essere scaricate, modificate e ripubblicate;
- il materiale postato online può permanervi per un tempo illimitato e potrebbe non essere mai definitivamente rimosso;
- esiste una distinzione ben delineata tra intimità e pubblicità.

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 miglior modo per prevenire casi di adescamento online è accompagnare i ragazzi in un percorso di autoaccettazione e di educazione (anche digitale) all'affettività.

Pertanto, per le classi terze della scuola secondaria di primo grado è previsto l'intervento dello psicologo, che aiuterà i ragazzi ad essere più sicuri emotivamente e pronti ad affrontare situazioni a rischio, imparando a gestire le proprie emozioni, il rapporto con il proprio corpo e con gli altri.

L'incontro con la Polizia Postale educherà studenti e genitori in merito alle pratiche di adescamento attraverso esperienze vissute, svolgendo opera di prevenzione in primis e fornendo in un secondo momento strumenti per tutelarsi.

Si rimanda, inoltre, al concetto di educazione digitale, che comprende anche lo sviluppo di capacità quali la protezione della propria privacy, la gestione dell'immagine e dell'identità online e l'adeguata gestione delle proprie relazioni online a partire dalla consapevolezza della peculiarità del mezzo tecnologico che permette a chiunque di potersi presentare molto diversamente da come realmente è.

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.

La questione della pedopornografia è estremamente delicata. Neanche in questo caso la scuola intende sostituirsi alla famiglia, ma si adopererà per collaborare con la stessa.

Se durante lo svolgimento delle attività didattiche si dovesse incorrere nel tema (articoli di attualità, ricerca di confronto da parte degli studenti), la scuola non si sottrarrà al suo compito educante. Il suo intervento sarà soprattutto volto a far capire la necessità di rivolgersi a un adulto quando qualcosa online mette a disagio.

Durante l'incontro con la Polizia Postale si informeranno studenti e genitori sui mezzi a disposizione per segnalare la diffusione di contenuti modificati non autorizzati e sugli strumenti di difesa personale da adottare.

Il nostro piano d'azioni

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

- Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti.
- Organizzare uno o più incontri di formazione all'utilizzo sicuro e consapevole di Internet e delle tecnologie digitali integrando lo svolgimento della didattica e assicurando la partecipazione attiva degli studenti.

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

- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti.
- Promuovere incontri e laboratori per studenti dedicati all'Educazione Civica

Digitale.

Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

Il personale docente del nostro Istituto quando ha il sospetto o la certezza che 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.

Il nostro istituto considera come infrazioni gravi i seguenti comportamenti accertati, che si configurano come forme di bullismo e cyberbullismo:

- insulti, termini volgari e offensivi tra studenti;

- ricorso alla violenza all'interno di una discussione;
- atti che mettono in pericolo l'incolumità altrui;
- danneggiamento volontario di attrezzature e strutture.

I suddetti comportamenti vengono considerati molto gravi qualora ripresi, diffusi e condivisi attraverso smartphone e tablet su social network, servizi di messaggeria, piattaforme, ecc.

Verrà inoltre segnalata la presenza di foto o video sessualmente espliciti nei dispositivi degli alunni, della scuola e nella rete, qualora se ne venga a conoscenza durante le attività didattiche.

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 segnalazione di casi sospetti ed evidenti avviene attraverso la compilazione di una specifica *SCHEDA DI SEGNALAZIONE* che deve essere sottoscritta dal segnalatore e non deve essere anonima.

Tale scheda va consegnata alla referente per la prevenzione e contrasto del bullismo e cyberbullismo, la quale a sua volta informa il Dirigente Scolastico.

5.3. - Gli attori sul territorio

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

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

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

- **Comitato Regionale Unicef**: laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni)**: svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare attenzione alla tutela dei minori.
- **Ufficio Scolastico Regionale**: supporta le scuole in attività di prevenzione ed anche nella segnalazione di comportamenti a rischio correlati all'uso di Internet.
- **Polizia Postale e delle Comunicazioni**: accoglie tutte le segnalazioni relative a comportamenti a rischio nell'utilizzo della Rete e che includono gli estremi del reato.
- **Aziende Sanitarie Locali**: forniscono supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in Rete. In alcune regioni, come il Lazio e

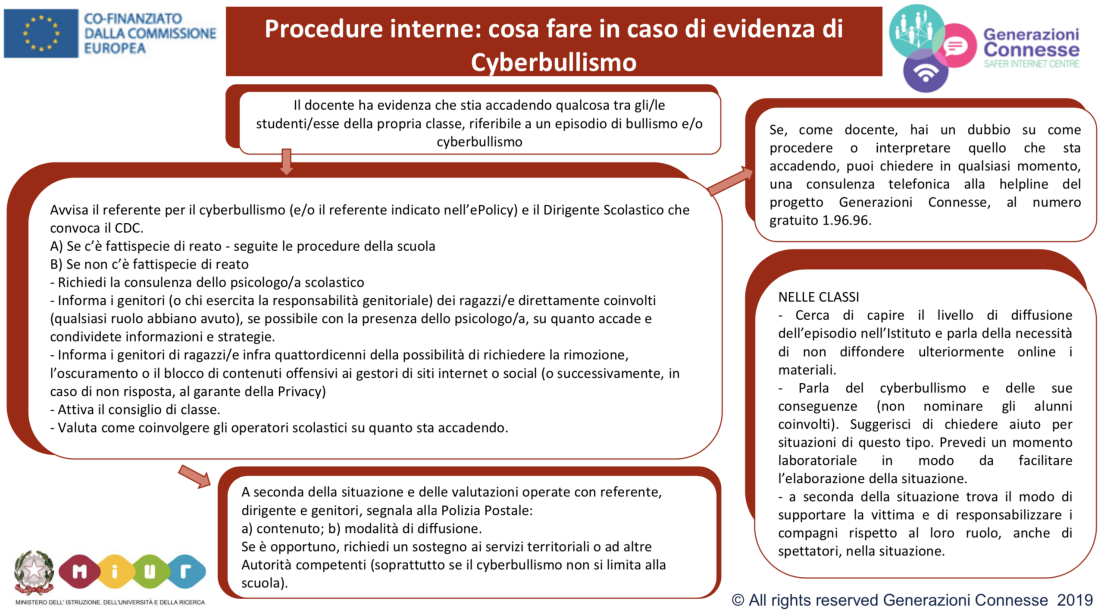
la Lombardia, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da Internet e alle situazioni di rischio correlate.

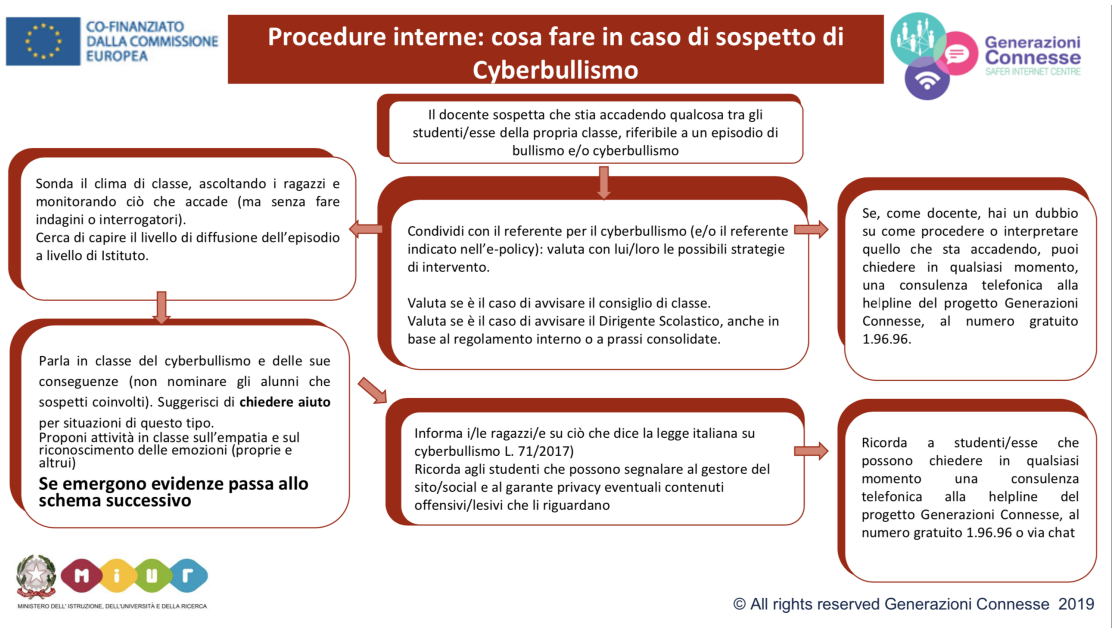
- **Garante Regionale per l'Infanzia e l'Adolescenza e Difensore Civico**: segnalano all'Autorità Giudiziaria e ai Servizi Sociali competenti; accolgono le segnalazioni di presunti abusi e forniscono informazioni sulle modalità di tutela e di esercizio dei diritti dei minori vittime. Segnalano alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.
- **Tribunale per i Minorenni**: segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

- Sindaco del Comune di Montegranaro
- Maresciallo dei Carabinieri
- Assistenti sociali
- Psicologo scolastico

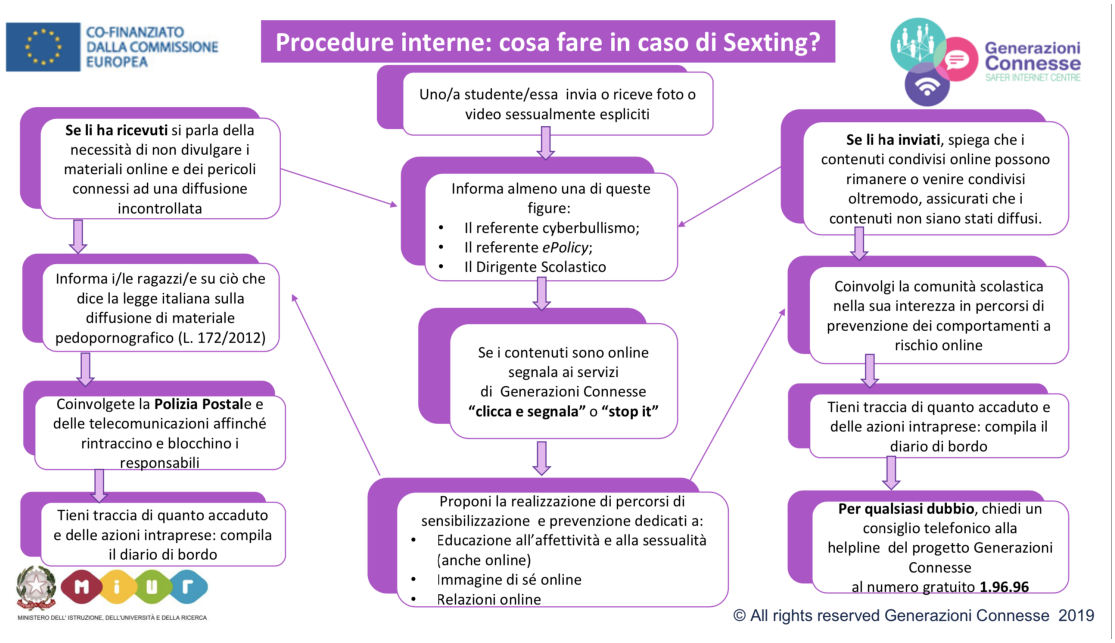
5.4. - Allegati con le procedure

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

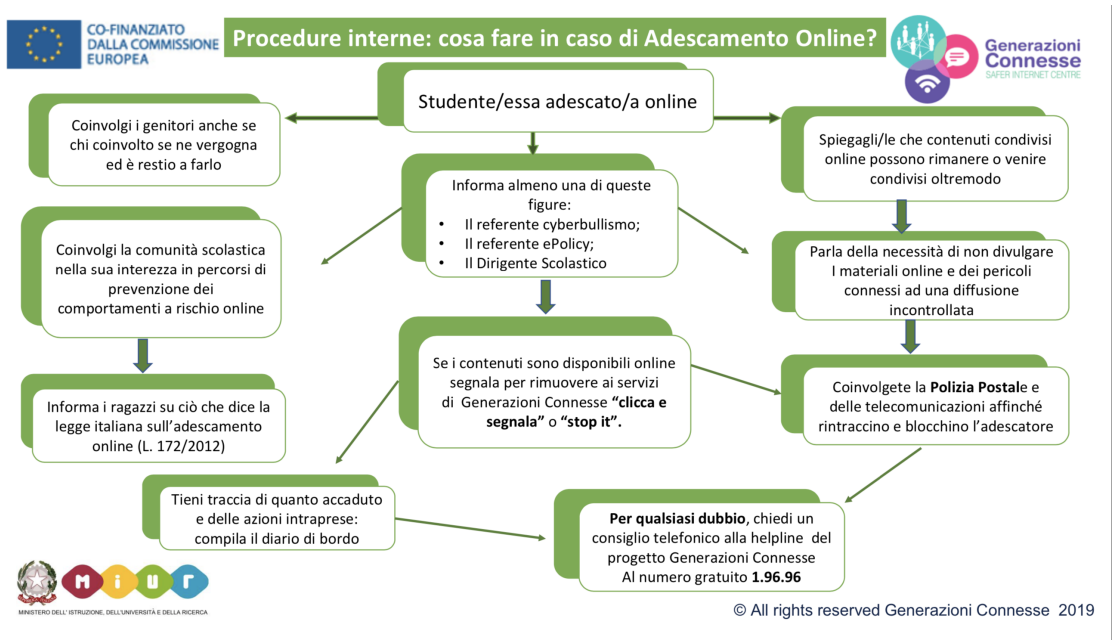




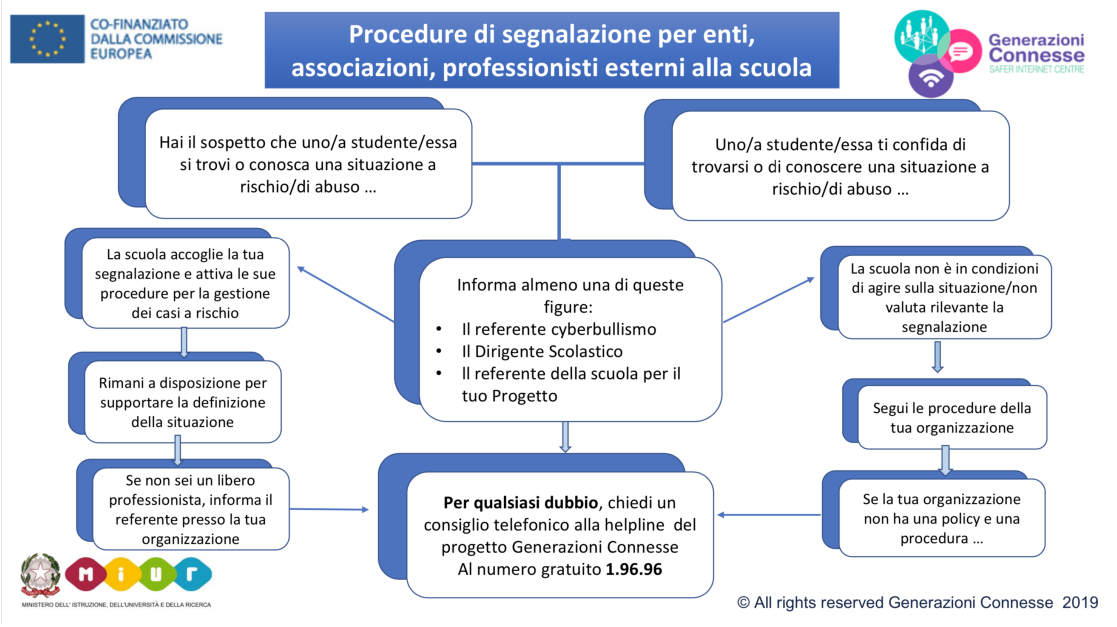
Procedure interne: cosa fare in caso di sexting?



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

La *SCHEDA DI SEGNALAZIONE* è all'interno del *Regolamento di prevenzione e contrasto del bullismo e cyberbullismo* del nostro istituto.

Il nostro piano d'azioni

Ogni anno la scuola si impegna a svolgere azioni di prevenzione e contrasto del bullismo e cyberbullismo attraverso incontri informativi e formativi per docenti, alunni e genitori.