Documento di ePolicy

RMIC8A400T

IC S.MARIA DELLE MOLE

VIA G. PRATI - 00040 - MARINO - ROMA (RM)

Paolino Giantruco

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.

L’e-.Policy è un documento volto a promuovere le competenze digitali ed un uso delle tecnologie digitali positivo, critico e consapevole sia da parte dei ragazzi e delle ragazze, che degli adulti coinvolti nel processo educativo.

Le Istituzioni Scolastiche devono avviare una politica di sicurezza della navigazione on line volta a un controllo dell’uso delle strumentazioni digitali e alla diffusione dell’adozione di buone pratiche di navigazione su Internet. Se bambini e giovanissimi mostrano un’innata predisposizione all’uso delle tecnologie, tuttavia, spesso a questa abilità non corrisponde un’adeguata e corretta capacità di gestione delle informazioni alla quale sono sottoposti .

L'autovalutazione e l’analisi dei bisogni che il nostro istituto ha realizzato sono fondamentali,inoltre, per la redazione dei PIANI DI AZIONE.

Dall’esigenza di questo bisogno di promozione di un uso sicuro e positivo delle tecnologie scaturisce il presente documento, prodotto dall’IC Santa Maria delle Mole, nell’ambito dell’adesione al 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.

In sintesi, il documento intende costituire un primo step in questa direzione e fornire alcune linee guida rispetto alle azioni dell’Istituto in ordine a:

• utilizzo consapevole delle TIC 1 in ambiente scolastico e nella didattica ;

• gestione di situazioni problematiche connesse all’uso delle tecnologie digitali.

Il documento potrà dunque, se necessario, essere modificato e aggiornato annualmente in funzione di eventuali nuove esigenze e, di conseguenza, di nuove azioni da porre in essere anche nell’ottica di una sua piena integrazione con obiettivi e contenuti degli altri documenti di Istituto, primo tra tutti il PTOF.

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.

Ruolo	Responsabilità
IL DIRIGENTE SCOLASTICO	• Responsabilità generale per i dati e la sicurezza degli stessi • Accertarsi che la scuola utilizzi un Internet Service filtrato approvato, conforme ai requisiti di legge vigenti • Responsabilità di assicurare che il personale riceva una formazione adeguata per svolgere i ruoli di sicurezza online e per la formazione di altri colleghi • Essere a conoscenza delle procedure da seguire in caso di infrazione della E-Safety Policy • Controllare e disporre aggiornamenti sulla E-Safety Policy • Ricevere relazioni di monitoraggio periodiche della sicurezza online da parte del responsabile • Gestire le segnalazioni ai Servizi Sociali • Monitorare l'utilizzo corretto di G-Suite

REFERENTE CONTRO IL BULLISMO E IL CYBERBULLISMO	• Coordinare le iniziative di prevenzione e di contrasto del cyberbullismo, anche avvalendosi della collaborazione delle Forze di polizia nonché delle associazioni e dei centri di aggregazione giovanile presenti sul Territorio (L. 71/2017, art. 4, c. 3) • Raccogliere e diffondere le buone pratiche educative, organizzative e azioni di monitoraggio. • Supportare il dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d'istituto), atti e documenti (PTOF, PdM, Rav). (Linee di orientamento) • Promuovere la consapevolezza e l'impegno per la salvaguardia online in tutta la comunità scolastica • Garantire che tutto il personale sia a conoscenza delle procedure che devono essere seguite in caso di incidente per la sicurezza online • Garantire che sia tenuto un registro di incidente di sicurezza online • Garantire la massima diffusione ai docenti, genitori e alunni, dei contenuti di prevenzione e contrasto ai fenomeni • Creazione di una mail apposita per le segnalazioni con apposito modulo • Facilitare la formazione e la consulenza per tutto il personale • Coordinare interventi con le autorità locali e le agenzie competenti • Facilitare la creazione di Reti significative e funzionali con il territorio • Raccordarsi con il Dirigente Scolastico e il suo staff • • Monitorare l'utilizzo corretto di G-Suite

L'ANIMATORE DIGITALE E IL TEAM	• Pubblicare la E-Safety Policy sul sito della scuola • Assistenza ai docenti per il controllo alla corretta navigazione • Diffusione delle netiquette sull'uso responsabile di internet • Diffusione della conoscenza di materiali per uso didattico in CC, Creative Commons e software open source. • Verifica dell'aggiornamento costante dell'antivirus e eliminazione applicazioni non autorizzate • Promuovere la formazione per i docenti e i genitori sulle tematiche in oggetto. • Amministrare, gestire e monitorare l'utilizzo corretto di G-Suite

GLI INSEGNANTI	• Inserire tematiche legate alla sicurezza online in tutti gli aspetti del programma di studi e di altre attività scolastiche • Supervisionare e guidare gli alunni con cura quando sono impegnati in attività di apprendimento che coinvolgono la tecnologia online • Garantire che gli alunni siano pienamente consapevoli delle capacità di ricerca e dei problemi legali relativi ai contenuti elettronici come ad esempio le leggi sul copyright. • Segnalare prontamente al Referente contro il bullismo e cyberbullismo, eventuali casi di cui si è venuto a conoscenza o se ne sospetta l'esistenza. • Formarsi sulle tematiche del cyberbullismo e della dipendenza da internet. • Diventare un punto di riferimento per i propri alunni in quanto a prevenzione, supporto e informazione. • Utilizzo corretto di G-suite e monitoraggio dell'uso da parte dei propri alunni.
IL PERSONALE SCOLASTICO	• Comprendere e contribuire a promuovere politiche di e-Safety • Essere consapevoli dei problemi di sicurezza online connessi con l'uso di telefoni cellulari, fotocamere e dispositivi portatili • Monitorare l'uso di dispositivi tecnologici e attuare politiche scolastiche per quanto riguarda questi dispositivi • Segnalare qualsiasi abuso sospetto o problema ai Responsabili di Plesso • Usare comportamenti sicuri, responsabili e professionali nell'uso delle tecnologie • Garantire che le comunicazioni digitali con gli studenti siano solo a livello professionale e solo attraverso sistemi scolastici, non attraverso chat o mail personali. • Utilizzo corretto di G-Suite

8

GLI ALUNNI	• Leggere, comprendere ed accettare la E-Safety Policy • Conoscere e rispettare le leggi sulla privacy e sul copyright • Capire l'importanza di segnalare abusi, minacce, atti di cyberbullismo o accesso a materiali inappropriati • Sapere quali azioni intraprendere se loro, o qualcuno che conoscono, si sente preoccupato o vulnerabile riguardo le nuove tecnologie • Conoscere e rispettare la politica della scuola relativa all'uso dei telefoni cellulari, tablet, fotocamere digitali e dispositivi portatili • Conoscere e capire la politica della scuola sull'uso di immagini e sul cyberbullismo • Capire l'importanza di adottare buone pratiche di sicurezza online quando si usano le tecnologie digitali fuori dalla scuola • Assumersi la responsabilità di conoscere i benefici e i rischi di utilizzo di internet e di altre tecnologie in modo sicuro,sia a scuola che a casa • Utilizzo corretto di G-Suite

9

I GENITORI	• Genitori e tutori svolgono un ruolo cruciale nel garantire che i loro figli comprendano la necessità di utilizzare i dispositivi Internet e mobili in modo appropriato. La scuola coglierà ogni occasione per sensibilizzare i genitori attraverso incontri con la Polizia postale ed altri esperti o educatori, circolari, sito web e altre comunicazioni telematiche, informazioni su campagne di sicurezza promosse da altre istituzioni o su convegni dedicati a questo tema. I genitori saranno incoraggiati a sostenere la scuola nel promuovere le buone pratiche di e-safety e a seguire le linee guida sull'uso appropriato di: o immagini digitali e video registrati in occasione di eventi scolastici, anche al di fuori delle aule; o accesso alle sezioni del sito dedicate ai genitori, con particolare riguardo al registro elettronico; o dispositivi personali dei loro figli nella scuola. • Monitorare l'utilizzo corretto di G-Suite dei propri figli.

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).

Tutti gli attori che entrano in relazione educativa con gli studenti e le studentesse devono: mantenere sempre un elevato profilo personale e professionale, eliminando atteggiamenti inappropriati, essere guidati dal principio di interesse superiore del

minore, ascoltare e prendere in seria considerazione le opinioni ed i desideri dei minori, soprattutto se preoccupati o allertati per qualcosa. Sono vietati i comportamenti irrispettosi, offensivi o lesivi della privacy, dell'intimità e degli spazi personali degli studenti e delle studentesse oltre che quelli legati a tollerare o partecipare a comportamenti di minori che sono illegali, o abusivi o che mettano a rischio la loro sicurezza. Tutti gli attori esterni sono tenuti a conoscere e rispettare le regole del nostro Istituto dove sono esplicitate le modalità di utilizzo dei propri dispositivi personali (smartphone, tablet, pc, etc.) e quelli in dotazione della scuola, evitando un uso improprio o comunque deontologicamente scorretto durante le attività con gli studenti e le studentesse. Esiste l'obbligo di rispettare la privacy, soprattutto dei soggetti minorenni, in termini di fotografie, immagini, video o scambio di contatti personali (numero, mail, chat, profili di social network). Gli Enti educativi esterni e le associazioni che entrano in relazione con la scuola devono conformarsi alla politica della stessa riguardo all'uso consapevole della Rete e delle TIC; devono, inoltre, promuovere comportamenti sicuri, la sicurezza online e assicurare la protezione degli studenti e delle studentesse durante le attività che si svolgono insieme

---

1.4 - Condivisione e comunicazione 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.

La E.Policy sarà pubblicata sulla Home Page del sito della scuola dopo essere stata approvata dal Collegio docenti.
All'inizio di ogni anno scolastico, insieme al Patto di Corresponsabilità Educativa, la E-Policy verrà illustrata ai genitori e agli alunni della scuola Primaria e Secondaria.

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.

Nel caso in cui una violazione al regolamento di istituto si configuri come atto di bullismo\cyberbullismo, colui che ne viene a conoscenza informa tempestivamente il il Dirigente Scolastico e il referente per il bullismo/cyberbullismo. Qualora tali infrazioni dovessero configurarsi come reato, il Dirigente Scolastico farà una tempestiva segnalazione all'autorità competente fatto obbligo di denuncia (ex art. 331 del Codice di Procedura Penale.

Si rinvia al Regolamento di Istituto e al Patto di Corresponsabilità

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 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 documento si integra pienamente con obiettivi e contenuti dei seguenti documenti: PTOFe del Regolamento interno.

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.

La E-Safety Policy sarà riesaminata ogni anno o quando si verificano cambiamenti significativi per quanto riguarda le tecnologie in uso all'interno della scuola e tutte le modifiche della Policy saranno discusse in dettaglio con tutti i membri del personale docenti.
La Policy è coerente con quanto previsto dalla legge 29 maggio 2017 n°71 "Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del Cyberbullismo "; dalla legge 31 dicembre 1996 n°675 "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali", dai Regolamenti vigenti di Istituto, e dal Patto di Corresponsabilità. Potrà essere integrata con il PTOF.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

- Creazione del gruppo di lavoro ePolicy (Azione sviluppabile nel breve periodo)
- Realizzazione di un sistema di monitoraggio delle attività (Azione sviluppabile nell'arco di un anno

Azioni da svolgere nei prossimi 3 anni:

Azione 1 (Azione sviluppabile nell'arco di un anno): Formazione del personale docente

Azione 2 (Azione sviluppabile nell'arco di tre anni): Incontri con consulenti esterni rivolti agli studenti, genitori, docenti e personale ATA relativamente al contrasto bullismo e cyberbllismo. scolastico):

Azione 3 (Azione sviluppabile alla fine di ogni anno scolastico): Restituzione del lavoro svolto da parte del Team al Collegio docenti

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.

Nell'ambito del PNSD questa scuola si propone un programma di progressiva educazione alla sicurezza online come parte del curriculum scolastico. Si impegna a sviluppare una serie di competenze e comportamenti adeguati all'età degli alunni e ad esperienza, tra cui:
• Programmare attività e far partecipare gli alunni a laboratori specifici sul digitale e la sicurezza in rete
• Sviluppare una serie di strategie per valutare e verificare le informazioni prima di accettare l'esattezza
• Essere a conoscenza delle fonti delle notizie in rete e che l'autore di un post o un sito web/pagina può avere un particolare pregiudizio
• Sapere come restringere o affinare una ricerca
• Riconoscere un comportamento accettabile quando si utilizza

un ambiente online, vale a dire, essere educato, non utilizzare comportamenti inappropriati, mantenere le informazioni personali private
• Conoscere e seguire la netiquette
• Capire come le fotografie possono essere manipolate e individuare contenuti web in grado di attrarre il tipo sbagliato di attenzione
• Comprendere l'esistenza e saper riconoscere i profili fake e le false identità degli interlocutori in chat e social network
• Capire il motivo per cui non dovrebbero inviare o condividere resoconti dettagliati delle loro vite personali e informazioni di contatto
• Capire il motivo per cui non devono pubblicare foto o video di altri senza permesso • Comprendere la motivazione del divieto di utilizzo dei cellulari a scuola
• Comprendere l'importanza di non scaricare file, software coperti da copyright o di dubbia natura
• Conoscere e contrastare i fenomeni di bullismo e cyberbullismo in tutte le sue forme.
• Sapere come chiedere aiuto e segnalare atti di bullismo e cyberbullismo
• Utilizzare con attenzione Internet per garantire che si adatti alla loro età e supporti gli obiettivi di apprendimento per le aree curricolari specifiche
• Conoscere e saper utilizzare positivamente le potenzialità delle nuove tecnologie e del mondo digitale.

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

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

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

È importante che tutti i docenti 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 ad ogni alunno modelli di utilizzo positivo, critico e specifico delle nuove tecnologie e per armonizzare gli apprendimenti. Per questo le TIC integrano la didattica per progettare, sviluppare, utilizzare, gestire e valutare i processi di insegnamento ed apprendimento di tutti gli studenti della classe compresi gli studenti con disabilità o DSA. Il fattore inclusivo di questa metodologia emerge così naturalmente. I docenti saranno pertanto invitati a seguire corsi di aggiornamento sulle tematiche digitali tramite seminari, workshop ricorrendo anche a consulenti esterni. Parte del personale docente provvede autonomamente ad integrare la formazione informatica proposta dall'istituto con corsi individuali sia online che in presenza nell'ottica della formazione

---

2.3 - Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali

La scuola si impegna a promuovere percorsi formativi per gli insegnanti sul tema dell'uso consapevole delle tecnologie digitali e della prevenzione dei rischi online. Ciò avverrà tramite specifici momenti di aggiornamento che, con cadenza, verranno organizzati dall'Istituto scolastico con la collaborazione del personale specializzato interno (animatore digitale, referente bullismo e cyberbullismo) e se necessario del personale esterno (professionisti qualificati), con il supporto della rete scolastica del territorio (USR, Osservatori regionali sul bullismo, scuole Polo, etc…), delle amministrazioni comunali, dei servizi socio-educativi e delle associazioni presenti.

Nell'ambito del PNSD questa scuola ha previsto:
• Individuazione e formazione di un Animatore Digitale che come docente accompagnerà il Dirigente Scolastico e il DSGA nell'attuazione degli obiettivi e delle innovazioni previste dal PNSD
• Formazione dei docenti all'utilizzo delle TIC, in particolare nell'utilizzo di G-Suite. • Assicurarsi che il personale sappia come inviare o ricevere dati sensibili o personali e comprendere l'obbligo di crittografare i dati dove la sensibilità richiede protezione degli stessi
• Offrire una formazione a disposizione del personale in materia di sicurezza online attraverso corsi di aggiornamento
• Fornire informazioni a tutto il nuovo personale circa le indicazioni presenti sulla E-Safety Policy d'Istituto.

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.

A partire dalla scuola primaria, la scuola invita i genitori ad assumersi l'incarico di accompagnare e supervisionare i figli durante la navigazione in rete, aiutandoli a riconoscere ed evitare i rischi .
Inoltre la scuola si assume i compiti di:
• Presentare ai genitori il Regolamento della Policy, al fine di garantire che i principi di comportamento sicuro online siano chiari
• Mettere a disposizione dei genitori e degli alunni una mail per informazioni, segnalazioni e supporto
• Gestire e aggiornare costantemente una sezione dedicata sul sito internet della scuola
• Fornire informazioni sui siti nazionali di sostegno per i genitori, quali il sito www.generazioniconnesse.it
• Fornire uno sportello di ascolto psicologico gratuito

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2021/22)

Scegliere almeno 1 di queste azioni

- 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.
- 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.

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

3.1 - Protezione dei dati personali

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

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

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

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

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

In questo paragrafo dell'ePolicy affrontiamo tale problematica, con particolare

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

L'istituto tratta solamente i dati personali necessari al perseguimento delle specifiche finalità istituzionali, oppure quelli espressamente previsti dalla normativa.

L'Istituto garantisce di trattare con estrema cautela e nel rispetto delle specifiche norme di legge i dati sensibili degli utenti. L'istituto emana una specifica informativa per normare l'acquisizione dei dati sensibili e richiede l'autorizzazione alle famiglie

. La Scuola adotta idonee misure tecniche organizzative per garantire la sicurezza del trattamento.

Al fine di migliorare la sicurezza e la protezione dei dati trattati, l'Istituto ha già compiuto la migrazione del sito da suffisso gov.it a suffisso edu.it.

Nel Regolamento Generale sulla Protezione dei Dati (Regolamento UE 2016/679) presente sul sito della scuola le famiglie, il personale scolastico, gli studenti possono conoscere tutte le disposizioni adottate in materia di protezione dati

---

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.

Questa scuola non pubblica indirizzi di posta elettronica personali degli alunni o del personale sul sito della scuola, eccezion fatta per mail istituzionali di area.

b. SITO WEB DELLA SCUOLA

Il sito dell'Istituto Comprensivo è raggiungibile all'indirizzo

http://www.icsmmole.edu.it/

Il Dirigente e lo staff verificano i contenuti destinati alla pubblicazione.

Responsabile della gestione del sito sono il D.S. , la funzione Strumentale in collaborazione con l'Animatore Digitale .

Al suo interno esiste una sezione dedicata alla tematica Bullismo/Cyberbullismo.

100. **SICUREZZA RETE LAN**

L'istituto , nella sede centrale, dispone di un dominio su rete locale (rete segreteria9 cui accedono i computer dell'amministrazione , tali postazioni sono una rete locale isolata dal resto della rete d'istituto(rete didattica). Una linea LAN è dedicata esclusivamente al computer del D.S.. Il collegamento di computer portatili o palmari personali alla rete d'istituto deve essere

autorizzato dal D.S..

- Tutte le sedi sono provviste di rete LAN.

- La rete interna è protetta da Firewall per quanto riguarda le connessioni con la rete

- Le postazioni sono protette con sistemi antivirus e antimalware regolarmente aggiornati.

- La memorizzazione dei documenti e delle impostazioni personali è garantita attraverso meccanismi di profili mobili di Window, che archivia centralmente sul server di dominio i dati, e li rende disponibili in tutte le postazioni legate alla didattica (laboratori, sale insegnanti, classi). Su questi dispositivi non è garantito alcun servizio di backup, pertanto si consiglia di fare copia su supporto personale.

SICUREZZA DELLA RETE SENZA FILI (WIRELESS- WIFI)

L 'Istituto , in tutti i suoi plessi , dispone di una rete con tecnologia senza fili. L'accesso alla rete wireless è regolamentato dalla chiave di accesso. L'ottenimento della chiave d'accesso è riservata solo agli autorizzati. Le regole di comportamento sono analoghe a quelle per la connessione alle reti cablate dell'istituto. L'istituto ha classi 2.0 e 3.0 e valuterà se utilizzare un sistema di Mobile Device Management con doppia funzionalità di controllo (a scuola attraverso un pannello di amministrazione dei docenti , a casa con le scelte dei genitori e/o tutori (scelta di app e di orari di utiliizzo)

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.

a. Email

Questa scuola ha predisposto per tutto il personale e per tutti gli alunni una mail istituzionale @icsantamariadellemole.edu.it fornito da G-Suite, che diventa l'unico canale autorizzato di invio comunicazioni tramite mail, eccezion fatta per la mail ufficiale rmic8a400t@istruzione .it

b. SITO WEB DELLA SCUOLA

Il sito dell'Istituto Comprensivo è raggiungibile all'indirizzo

http://www.icsmmole.edu.it/

Il Dirigente e lo staff verificano i contenuti destinati alla pubblicazione.

Responsabile della gestione del sito sono il D.S. , la funzione Strumentale in collaborazione con l'Animatore Digitale Al suo interno esiste una sezione dedicata alla tematica Bullismo/Cyberbullismo.

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.

STRUMENTAZIONE PERSONALE

a. Per gli studenti. Gestione degli strumenti personali

Come da Regolamento d'Istituto agli studenti è vietato l'utilizzo del cellulare

all'interno della scuola , salvo dietro espresso permesso del docente e per soli

fini didattici che andranno relazionati e documentati. Per quanto concerne

l'utilizzo del tablet o del pc, questi possono essere utilizzati in presenza del

docente e per ragioni prettamente didattiche.

b. PER I DOCENTI E PER IL PERSONALE DELLA SCUOLA : GESTIONE DEGLI

STRUMENTI PERSONALI

I docenti e il personale della scuola possono utilizzare smartphone e tablet

esclusivamente a fini didattici e istituzionali (compilazione del Registro Elettronico

ricerche didattiche, consultazione siti istituzionali , ecc.)

Il personale della scuola, dietro richiesta motivata dapresentare al DS e solo dopo

autorizzazione tale richiesta può ottenere un voucher di accesso alla rete Internet

dell'istituto.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2021/2022).

Scegliere almeno 1 di queste azioni:

- Effettuare un’analisi sull’utilizzo dei dispositivi personali a scuola da parte deglistudenti e delle studentesse
- 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 personal

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 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)

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.*

lL'Istituto si impegna a svolgere un'attività di prevenzione e sensibilizzazione sulle tematiche del:

- Cyberbullismo

-Hate speech

-Dipendenza da Internet e gioco online

-Sexting

-Adescamento online

- Pedopornografia

A tal proposito saranno privilegiati gli interventi del referente bullismo e della relativa commissione che trattino le suddette tematiche e sarà intensificata la collaborazione con le forze dell'ordine impegnate nella prevenzione dei rischi e dei reati connessi all'uso improprio della rete.

L'Istituto e i docenti si impegnano altresì a diffondere e promuovere tra gli studenti e le famiglie la conoscenza della piattaforma "Generazioni connesse" inserendo sul sito web istituzionale il link del progetto: www.generazioniconnesse.it, dove trovare ulteriori approfondimenti, spunti, aggiornamenti e strumenti didattici utili.

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).

Gli atti di cyberbullismo possono essere suddivisi in due gruppi:

-diretto: il bullo utilizza strumenti di messaggistica istantanea come SMS o MMS, che hanno un effetto immediato sulla vittima poiché diretti esclusivamente alla persona;

-indiretto: il bullo fa uso di spazi pubblici della Rete, come Social network, blog o forum, per diffondere contenuti dannosi e diffamatori per la vittima. Tali contenuti possono diventare virali e quindi più pericolosi per la vittima, anche dal punto di vista psicologico.

Indicatori di segnali che può manifestare una potenziale vittima di cyberbullismo sono:

-Appare nervosa quando riceve un messaggio o una notifica;

-Sembra a disagio nell'andare a scuola o finge di essere malata (ha spesso mal di stomaco o mal di testa);

-Cambia comportamento ed atteggiamento in modo repentino;

-Mostra ritrosia nel dare informazioni su ciò che fa online;

-Soprattutto dopo essere stata online, mostra rabbia o si sente depressa;

-Inizia ad utilizzare sempre meno PC e telefono (arrivando ad evitarli);

-Perde interesse per le attività familiari o per le attività extra-scolastiche che prima svolgeva;

-Il suo rendimento scolastico peggiora.

La scuola si impegna a :

- Riconoscere il D.S. Come titolare del trattamento di dati personali secondo la GDP art. 28 e al D. Lgs. 10 Agosto 2018, n101
- Riconoscere come tutori della sicurezza online il DSGA, l'Animatore Digitale, la FS e il Team Digitale;
- Rendere aggiornata e attiva la Piattaforma G-Suite

I docenti si impegnano a:

- Accompagnare gli alunni nella navigazione in Rete, coinvolgendoli nell' esplorare delle opportunità e dei rischi, con attività calendarizzate dall'inizio dell'anno
- Sostenere gli alunni nel corretto uso della paittaforma di G-Suite
- Approfondire con attività mirate in classe, la conoscenza del fenomeno del bullismo e del cyberbullismo (suggerimenti e materiale proposti dal Team antibullismo).

  Creare degli spazi in cui gli alunni si possano confrontare su questo tema, utilizzando come spunti di riflessione: film, video, canzoni, incontri con esperti, letture mirate, lavori di gruppo sulle tematiche (suggerimenti e materiale proposti dal Team antibullismo).
- Riferirsi al Referente contro il Bullismo e il Cyberbullismo per le tematiche in oggetto
- Rivolgersi alla helpline di generazioni connessse www.generazioniconnesse.it
- Il Referente Cyberbullismo propone attività e riflessioni per la giornata del "Safer Internet Day ", pubblicizza eventi esterni cui possono partecipare i ragazzi accompagnati dai docenti.

I GENITORI SI IMPEGNANO A :

-Firmare il Patto di Corresponsabilità redatto dalla scuola

- Prendere visione della E-safety Policy messa a disposizione di docenti, genitori ed alunni sul sito della scuola www.icsmmole.edu.it
- Seguire le azioni promosse dalla scuola per un uso corretto della rete
- Frequentare corsi di formazione /convegni che la scuola organizzerà per la diffusione di informazioni legate ad un uso corretto della tecnologia digitale.
- Controllare l'utilizzo responsabile dei servizi di messaggistica istantanea dei propri figli .

Sostenere i propri figli nell' utilzzo corretto di G-Suite.

GLI ALUNNI SI IMPEGNANO A :

- Prendere visione del Patto di Corresponsabiltà che i genitori hanno firmato con la scuola.

Prendere visione della E-Safety Policy pubblicata sul sito della scuola

- Rispettare le regole per un uso corretto delle tecnologie digitali.
- Utilizzare correttamente la piattaforma G-Suite, seguendo srupolosa-mente il Regolamento d' uso e e indicazioni fornite dal proprio insegnante.
- Denunciare qualsiasi caso di abuso online.
- Prendere parte a qualsiasi evento che la scuola organizza in materia di sicurezza online.

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

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

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

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

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

Il referente bullismo e il team antibullismo terranno una serie di incontri con gli studenti e le studentesse dei diversi gradi di istruzione per sensibilizzarli su questo tema così importante allo scopo di far maturare in loro la consapevolezza di sé e dell'altro e l'importanza del rispetto reciproco.Inoltre ogni docente, all'interno delle sue discipline e delle sue ore con gli studenti e le studentesse, dedica tempo ed energie alla costruzione di un ascolto attivo e di un dialogo pacifico.

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?

L’istituto è intenzionato a promuovere azioni di prevenzione attraverso percorsi sul benessere digitale e a creare degli spazi in cui gli alunni si possano confrontare su

questo tema, utilizzando come spunti di riflessione: film, video, canzoni, incontri con esperti, letture mirate, lavori di gruppo sulle tematiche (suggerimenti e materiale proposti dal Team antibullismo .

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.

Sono in fase di progettazione per il prossimo anno scolastico le azioni che il nostro Istituto intende intraprendere per prevenire ed affrontare la delicata problematica dell’adescamento.

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 refente bullismo e il team antibullismo creeranno degli spazi in cui gli alunni si possano confrontare su questo tema, utilizzando come spunti di riflessione: film, video, canzoni, letture mirate, lavori di gruppo sulla tematica in oggetto

---

4.7 - Pedopornografia

La pedopornografia online è un reato (art. 600-ter comma 3 del c.p.) che consiste nel produrre, divulgare, diffondere e pubblicizzare, anche per via telematica, immagini o video ritraenti bambini/e, ragazzi/e coinvolti/e in comportamenti sessualmente espliciti, **concrete o simulate** o qualsiasi rappresentazione degli organi sessuali a fini soprattutto sessuali.

La legge n. 269 del 3 agosto 1998 *"Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di schiavitù", introduce nuove fattispecie di reato (come ad esempio il turismo sessuale) e, insieme alle successive modifiche e integrazioni contenute nella* ***legge n. 38 del 6 febbraio 2006*** *"Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet"*, segna una tappa fondamentale nella definizione e predisposizione di strumenti utili a contrastare i fenomeni di sfruttamento sessuale a danno di minori. Quest'ultima, introduce, tra le altre cose, il reato di "pornografia minorile virtuale" (artt. 600 ter e 600 quater c.p.) che si verifica quando il materiale pedopornografico rappresenta immagini relative a bambini/e ed adolescenti, realizzate con tecniche di elaborazione grafica non associate, in tutto o in parte, a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali.

Secondo la Legge 172/2012 - *Ratifica della Convenzione di Lanzarote (Art 4.) per pornografia minorile si intende ogni rappresentazione, con qualunque mezzo, di un minore degli anni diciotto coinvolto in attività sessuali esplicite, reali o simulate, o qualunque rappresentazione degli organi sessuali di un minore di anni diciotto per scopi sessuali.*

In un'ottica di attività preventive, il tema della pedopornografia è estremamente delicato, occorre parlarne sempre in considerazione della maturità, della fascia d'età e selezionando il tipo di informazioni che si possono condividere.

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

Inoltre, è auspicabile che possa rientrare nei temi di un'attività di sensibilizzazione rivolta ai genitori e al personale scolastico promuovendo i servizi di Generazioni Connesse: qualora navigando in Rete si incontri materiale pedopornografico è opportuno segnalarlo, anche anonimamente, attraverso il sito www.generazioniconnesse.it alla sezione **"Segnala contenuti illegali"** (Hotline).

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

IL refente bullismo e il team antibullismo proporranno agli alunni degli incontri su questo tema così delicato .

I docenti a loro volta utilizzeranno come spunti di riflessione: film, video, canzoni, letture mirate, lavori di gruppo sulla tematica in oggetto .

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2021/2022).

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.

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.

☐ Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai ai docenti, con il coinvolgimento di esperti.

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.

Vanno segnalate tutte le azioni che possono far pensare che un nostro alunno sia vittima di bullismo, ciberbullismo, sexting, adescamento on-line e pedopornografia.

Tali situazioni possono essere riferite direttamente da chi l'ha subita, da un compagno di classe, da un docente , da un genitore che ne è a conoscenza.

Vanno altresì segnalate nello stesso modo , le situazioni in cui un alunno sia autore di sexting, adescamento on-line, cyberbullismo o di azioni considerate inadeguate o lesive dei diritti altrui.

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.

Nel caso in cui il docente si trovi di fronte ad una situazione in cui sospetta che stia avvenendo qualcosa tra gli alunni della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online oppure abbia la certezza che stia accadendo qualcosa tra gli studenti della propria classe deve agire immediatamente rispettando il protocollo stabilito.

- Nel CASO SOSPETTO il docente si rivolge immediatamente al Referente Bullismo ed insieme valutano le possibili strategie d'intervento. A seconda della portata dell'accaduto, il docente può inoltre avvisare l'intero consiglio di classe e, se si ravvisa la necessità, coinvolgere il Dirigente Scolastico. Nel frattempo, il docente e i docenti informati ascoltano gli studenti e le studentesse, osservando e monitorando il clima di classe, ciò che accade e le dinamiche relazionali nel contesto classe, senza fare indagini dirette.

- Nel CASO EVIDENTE, il docente condivide immediatamente quanto osservato con il referente per il bullismo che valuta le possibili strategie di intervento. Si avvisa il Dirigente Scolastico che convoca il consiglio di classe. Se non si ravvisano fattispecie di reato, si procede nel seguente modo:

-si informano i genitori (o chi esercita la responsabilità genitoriale) degli/delle studenti/studentesse direttamente coinvolti/e (qualsiasi ruolo abbiano avuto) su quanto accaduto e si condividono informazioni e strategie;

-si richiede , ove fosse necessario,la consulenza dello psicologo scolastico a supporto della gestione della situazione,,

-in base alla gravità dell'accaduto; effettuate con referente, dirigente e genitori, si valuta la segnalazione alla Polizia Postale delle seguenti informazioni: a) contenuto del materiale online offensivo b) modalità di diffusione c) fattispecie di reato Internet

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

-un indirizzo e-mail specifico per le segnalazioni;

- sportello di ascolto con professionisti;

-docente referente per le segnalazioni.

Gli studenti e le studentesse, infine, possono rivolgersi alla Helpline del progetto Generazioni Connessee al numero gratuito 1.96.96.

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.

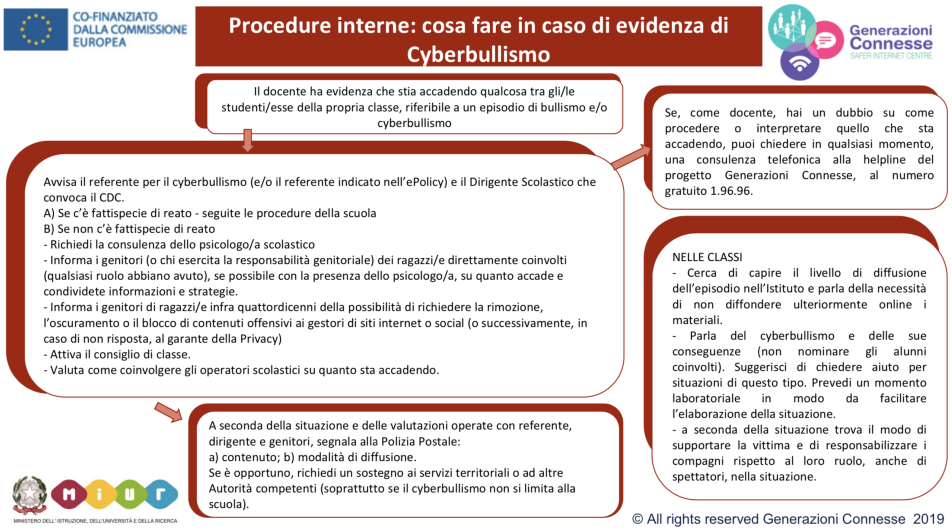
- **Tribunale per i Minorenni**: segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

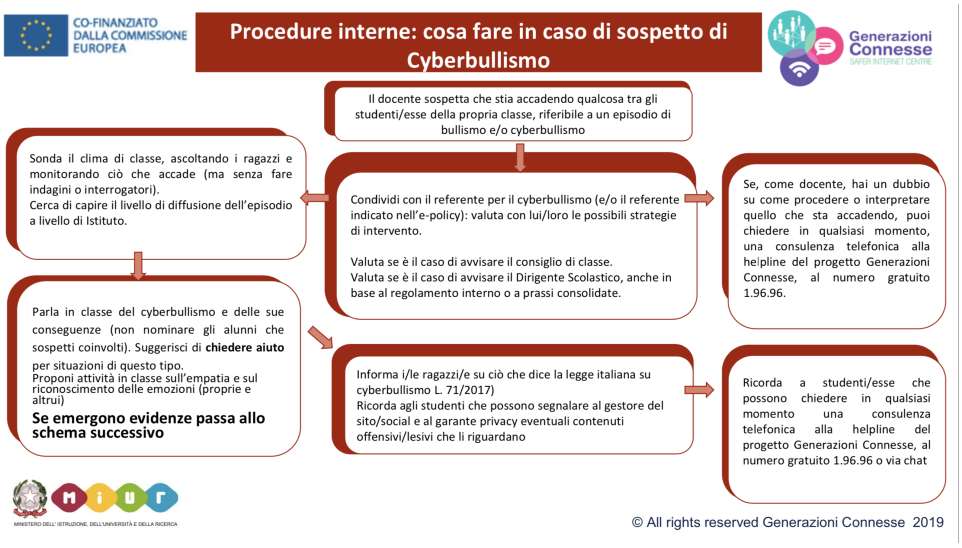
- Servizi sociali comunali e di Ambito

- Agenzie educative del territorio

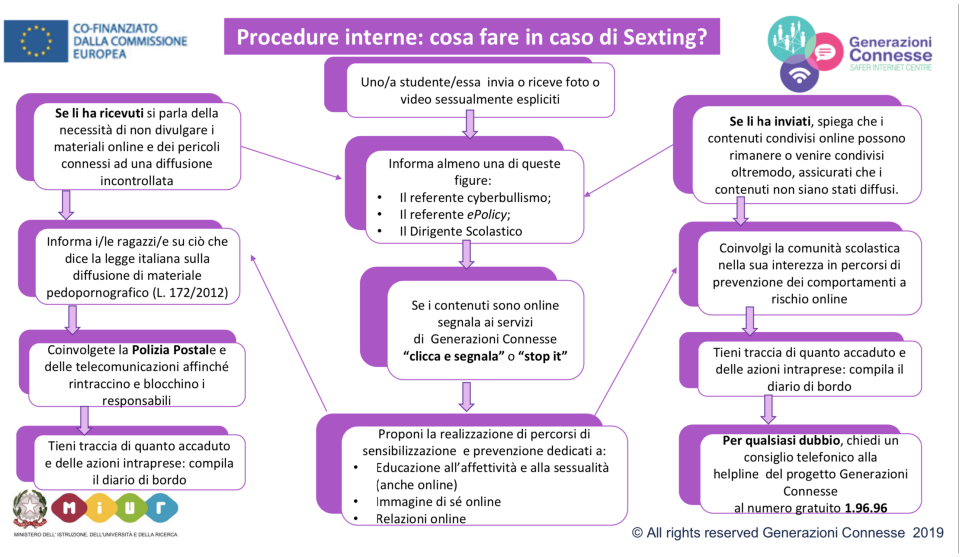
5.4. - Allegati con le procedure

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

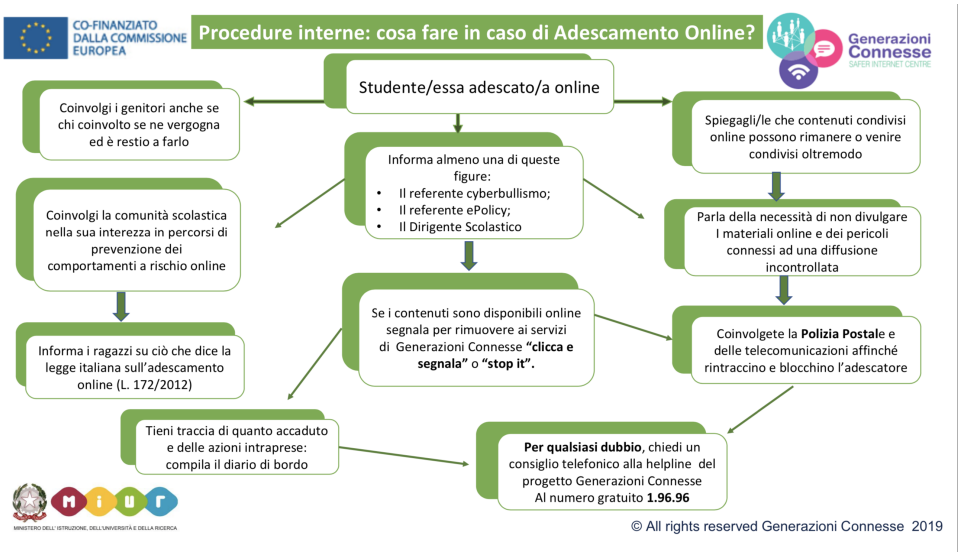




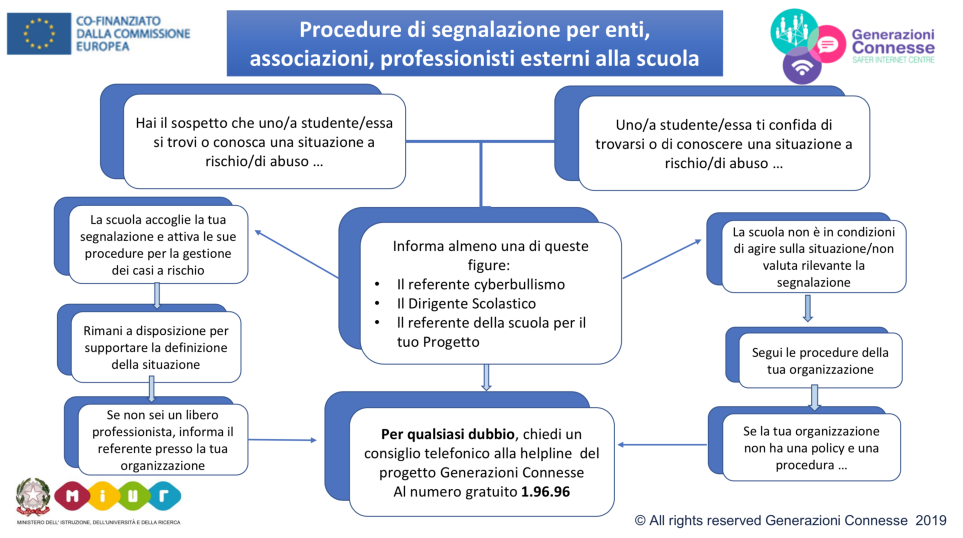
Procedure interne: cosa fare in caso di sexting?



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

1. **Questionario di automonitoraggio sulle segnalazioni**
2. **Strutturazione della procedura di prima sgnalazione**
3. **Ricognizione delle risorse umane**
4. **Modulo prima segnalazione dei casi di (presunto) Bullismo o Cyberbullismo**
5. **Valutazione approfondita dei casi di B. / vittima**
6. **Intervento di rete con il territorio**
7. **Scheda di monitoraggio**
8. **Costruisci il lancio del protocollo nella tua scuola**

Il nostro piano d'azioni

RILEVAZIONE E GESTIONE DEI CASI

La scuola si impegna ad organizzare le seguenti attività di prevenzione al fenomeno:

- Organizzazione di Corsi di formazione per docenti, genitori ,personale scolastico

- Monitoraggio sul tema del cyberbullismo attraverso il questionario al link

https://docs.google.com/forms/d/e/1FAIpQLScSvTnzS1OVTTddeOBqET75lrBCOus- WLDJ_RpwPW736FHwjg/viewform?usp=pp_url

-Partecipazione da parte di docenti, studenti e genitori a convegni e seminari sul tema del bullismo e cyberbullismo

- Supporto psicologico ad alunni, genitori e docenti (Sportello d'ascolto)

PROCEDURE OPERATiVE PER LA GESTIONE DELLE INFRAZIONI ALLA POLICY

La scuola dopo aver preso visione ed analizzato le procedure per la rilevazione , il monitoraggio e la gestione delle segnalazioni procede con l'iter in caso di presunto B./Cyb. o Vittimizzazione .

ITER:

PRIMA SEGNALAZIONE (1)

VALUTAZIONE APPROFONDITA (2)

GESTIONE CASO ATTRAVERSO UNO o PIU' INTERVENTI (3):

APPROCCIO EDUCATIVO CON LA CLASSE (3.1)

INTERVENTO INDIVIDUALE (3.2)

GESTIONE DELLA RELAZIONE (3.3)

COINVOLGERE LA FAMIGLIA (3.4)

SUPPORTO INTENSIVO A LUNGO TERMINE E DI RETE (3.5)

ACCOGLIERE LA SEGNALAZIONE :

1. **Modulo di prima segnalazione**
2. **Lancio del protocollo**
3. **Valutazione approfondita**

GLI INTERVENTI :

dopo la valutazione , in base alla gravità si assegna un codice

Codice verde : Situazione da monitorare con interventi in classe (3.1)

Codice giallo : Interventi indicati e strutturati a scuola e in sequenza in rete se non ci sono risultati (3.1), (3.2), (3.3), (3.4)

Codice rosso : Interventi di emergenza con supporto della rete (3.2), (3.4), (3.5).

MONITORAGGIO (MODULO PER IL MONITORAGGIO DEI CASI

SEGNALATI E PRESA IN CARICO).

PROCEDURE OPERATIVE PER LA RILEVAZIONE , IL MONITORAGGIO E LA GESTIONE DELLE SEGNALAZIONI