ISTITUTO D'ISTRUZIONE SUPERIORE " GRAZIO COSSALI "

Protocollo numero: ***1546 / 2023***
Data registrazione: ***31/01/2023***

Tipo Protocollo: ***USCITA***
Documento protocollato: ***Documento_E-Policy31_01_2023-11_11_24.pdf***
IPA: ***istsc_bsis01300g***

Oggetto: ***Documento di e-Policy***

Destinatario:
GENERAZIONI CONNESSE

Ufficio/Assegnatario:
DIRIGENTE SCOLASTICO

Protocollato in:
4993 - REGOLAMENTI
Titolo: ***2 - ORGANI E ORGANISMI***
Classe: ***5 - Dirigente scolastico DS***
Sottoclasse: ***- - -***

COPIA CONFORME ALL'ORIGINALE DIGITALE

Documento di ePolicy

BSIS01300G

"COSSALI" - ORZINUOVI

VIA MILANO 83 - 25034 - ORZINUOVI - BRESCIA (BS)

Luca Alessandri

Capitolo 1 - Introduzione al documento di ePolicy

1.1 - Scopo dell'ePolicy

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

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

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

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

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

Argomenti del Documento

Perché è importante dotarsi di una E-policy?

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

all’uso di Internet.

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

Tale documento avrà, quindi, lo scopo di fornire all'intera comunità scolastica le linee guida per un uso consapevole e critico delle tecnologie digitali e di Internet, seguendo le indicazioni di Educazione Civica Digitale emanate dal MIM, per:

- salvaguardare e proteggere gli studenti e tutto il personale dell’Istituto;
- assistere il personale della scuola a lavorare in modo sicuro e responsabile;
- impostare chiare aspettative di comportamento e/o codici di condotta rilevanti per un uso responsabile di Internet a scopo didattico, personale o ricreativo;
- affrontare gli abusi online come il cyberbullismo;
- garantire che tutti i membri della comunità scolastica siano consapevoli del fatto che il comportamento illecito o pericoloso è inaccettabile e che saranno intraprese le opportune azioni disciplinari e giudiziarie.

Il testo integra le indicazioni contenute nei seguenti documenti:

- Regolamento di Istituto;
- Regolamento antibullismo;
- Piano triennale di attuazione del PNSD;
- Patto di corresponsabilità;
- Piano Triennale dell'Offerta Formativa;

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.

DIRIGENTE SCOLASTICO

Il Dirigente scolastico è garante per la sicurezza di tutti i membri della comunità scolastica. Promuove ed attiva buone prassi secondo il quadro normativo di riferimento e le indicazioni del MIM, mediante l'organizzazione di percorsi di formazione specifici per tutte le figure scolastiche sull'utilizzo positivo e responsabile delle TIC e sulle problematiche connesse all'utilizzo della rete sia online che offline. Il Dirigente, coadiuvato dal Team per l'emergenza del Bullismo e del Cyberbullismo, ha inoltre la

responsabilità di gestire ed intervenire nei casi di gravi episodi di bullismo, cyberbullismo e di uso improprio delle tecnologie digitali.

ANIMATORE DIGITALE

L'animatore digitale rappresenta un valido supporto per l'intero personale scolastico non solo dal punto di vista tecnico-informatico, ma anche in riferimento alla protezione e gestione dei dati personali, rischi online, e per buone prassi in materia di percorsi di formazione "scuola digitale" ed "educazione civica". Inoltre monitora e rileva eventuali episodi o problematiche connesse all'uso delle TIC a scuola, e ha il compito di controllare che gli utenti autorizzati accedano alla Rete della scuola con apposita password, per scopi istituzionali e consentiti (istruzione e formazione).

REFERENTE DEL BULLISMO E DEL CYBERBULLISMO

"Ogni Istituto scolastico, nell'ambito della propria autonomia, individua fra i docenti un referente con il compito di coordinare le iniziative di prevenzione e di contrasto del cyberbullismo" (Art. 4 Legge n.71/2017, "Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo" (permalink – file 1 LEGGE 71_2017 in allegato). Tale figura ha il compito di coordinare il team specializzato per la gestione dei casi di bullismo e cyberbullismo; collaborare con i servizi del territorio; curare le relazioni con la famiglia; progettare attività informative e formative rivolte agli studenti e alle loro famiglie in merito al tema del bullismo e del cyberbullismo, all'uso consapevole della tecnologia, al potenziamento delle abilità socio-affettive, alla legalità e al rispetto della dignità personale di ognuno.

DOCENTI

I Docenti hanno un ruolo centrale nel diffondere la cultura dell'uso responsabile delle TIC e della Rete. Promuovono, laddove possibile, l'uso delle tecnologie digitali nella didattica. Accompagnano e supportano gli studenti e le studentesse nelle attività di apprendimento e nei laboratori che prevedono l'uso dei vari dispositivi tecnologici che si connettono alla Rete; hanno il dovere morale e professionale di segnalare al Dirigente Scolastico qualunque problematica, violazione o abuso, anche online, che vede coinvolti studenti e studentesse.

PERSONALE AMMINISTRATIVO, TECNICO E AUSILIARIO (ATA)

Il personale non docente, svolge funzioni di tipo amministrativo, contabile, gestionale e di sorveglianza, connesse alle attività dell'Istituto, in collaborazione con il Dirigente Scolastico e con tutto il personale docente. È coinvolto nella segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo insieme alle figure interne preposte.

STUDENTI E STUDENTESSE

Gli studenti e le studentesse sono tenuti/e al rispetto delle norme che disciplinano

l'utilizzo consapevole delle tecnologie digitali con la finalità di salvaguardare la propria identità e quella altrui, secondo quanto indicato nel Regolamento d'Istituto. La partecipazione a percorsi formativi e progettuali ha lo scopo di promuovere l'utilizzo positivo delle TIC e della Rete, eventulamente anche in una dimensione di peer education.

GENITORI

I Genitori sono corresponsabili nelle scelte educative dell'Istituzione scolastica, atte alle attività di prevenzione ed uso consapevole delle TIC, della Rete e dei device personali dei rispettivi figli. Ad essi è richiesto di sostenere i docenti nell'azione educativa diretta al corretto utilizzo delle tecnologie digitali vigilando sui propri figli in ambiente domestico fissando regole comportamentali, in particolare in caso di attività di didattica a distanza. Infine sono sollecitati a collaborare con i docenti nell'adozione di linee di intervento coerenti per contrastare l'uso non responsabile, scorretto o pericoloso delle tecnologie digitali.

ENTI EDUCATIVI ESTERNI E ASSOCIAZIONI

Gli enti educativi esterni e le Associazioni che entrano in relazione con l'Istituto, osservano le politiche interne sull'uso consapevole della Rete e delle TIC. Durante le attività che svolgeranno all'interno della scuola attiveranno le procedure e i comportamenti sicuri per la protezione e la sicurezza degli studenti e delle studentesse.

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).

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;
- promuovere comportamenti sicuri e assicurare la protezione degli studenti e delle studentesse durante le attività che vengono svolte in Istituto.
- segnalare attraverso le modalità e gli strumenti che l'Istituto mette a disposizione, come indicato nel punto 1.5 del presente documento, atteggiamanti, atti e azioni, che destino sospetto e violino il codice di comportamento da parte degli studenti e delle studentesse.

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.

Il testo, approvato dal Collegio docenti e dal Consiglio d'Istituto, è comunicato all'intera comunità scolastica attraverso la pubblicazione sul sito della scuola, nella sezione Regolamenti.

L'E-Policy d'Istituto viene, inoltre, condiviso

- con i docenti attraverso la discussione e l'approvazione in ambito collegiale dei contenuti, delle pratiche e dei protocolli di intervento;
- con la componente studentesca attraverso: la discussione in classe con il coordinatore o personale formato sulla policy, nei primi giorni di attività scolastica, con particolare riguardo al protocollo di accoglienza per le nuove classi prime; la diffusione tra gli studenti di un estratto del documento relativo, in particolare, ai comportamenti da attuare in caso di bisogno; la lettura, comprensione e sottoscrizione del Patto di Corresponsabilità.

1.5 - Gestione delle infrazioni alla ePolicy

La scuola gestirà le infrazioni all'E-policy attraverso azioni educative e/o sanzioni, qualora fossero necessarie, valutando i diversi gradi di gravità di eventuali violazioni.

L'Istituto ritiene di fondamentale importanza, in situazioni di infrazioni alla E-Policy, intervenire su tutto il contesto classe con attività specifiche educative e di sensibilizzazione, gestite dai docenti o da professionisti esterni, per promuovere una maggiore consapevolezza e mantenere un clima di classe attivo, responsabile e aperto alla gestione dei conflitti.

Tutte le infrazioni o qualsiasi sospetto, rischio, violazione andranno tempestivamente segnalate al Team dell'emergenza per il bullismo e alle altre figure interessate che riferiranno al Dirigente Scolastico, il quale avrà cura di convocare le parti interessate onde valutare le possibili azioni da intraprendere.

La scuola procederà secondo quanto previsto dal Regolamento di Istituto degli studenti (pubblicato sul sito web dell'istituto) in uno spirito di accoglienza, recupero ed educazione, valutando la natura e la gravità di quanto accaduto, al fine di considerare la necessità di denunciare l'episodio è/o di garantire immediato supporto psicologico allo/la studente/ssa attraverso i servizi predisposti (Sportello psicologico, Sportello di

mediazione e gestione dei conflitti), previo consenso del genitore.

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.

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.

L'eventuale revisione, aggiornamento e implementazione del testo saranno a carico del gruppo di lavoro che ha redatto il documento.

Il nostro piano d'azioni

Azioni da svolgere durante l'anno scolastico in corso:

- Presentare il progetto e consultare i docenti dell'Istituto per la stesura finale dell'ePolicy.

Azioni da svolgere durante l'anno scolastico 2023/2024:

- Organizzare un incontro per la consultazione dei rappresentanti degli studenti/studentesse sui temi dell'ePolicy per cui si evidenzia la necessità di regolamentare azioni e comportamenti.

- Sensibilizzare la comunità scolastica sull'adozione di misure di prevenzione e sulla gestione di situazioni problematiche relative all'uso delle TIC.
- Avviare la stesura di progetti sulla Legalità, sulle Competenze Digitali, sulla Cittadinanza attiva, sul contrasto al bullismo e cyber bullismo.

Azioni da svolgere nei 3 anni successivi:

- Organizzare dei momenti di confronto tra gli studenti, nell'ambito del Progetto Accoglienza e di Educazione Civica, sui temi dell'e-Policy.
- Sensibilizzare la comunità scolastica sull'adozione di misure di prevenzione e sulla gestione di situazioni problematiche relative all'uso delle TIC.
- Sviluppare dei progetti sulla Legalità, sulle competenze digitali, sulla Cittadinanza attiva, sul contrasto al bullismo e cyber bullismo con la collaborazione di soggetti esterni che si occupano a vario titolo dell'educazione dei ragazzi/e.
- Somministrare agli studenti e studentesse un questionario on line volto a segnalare comportamenti non adeguati.

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.

Quando si parla di competenze digitali è necessario integrare la dimensione tecnologica con quella cognitiva ed etica:

- dimensione tecnologica: prevede la riflessione sul potenziale delle tecnologie digitali, intese come strumenti per la risoluzione di problemi della vita quotidiana, onde evitare automatismi che abbiano conseguenze incerte, attraverso un'adeguata comprensione della "grammatica" dello strumento, per selezionare di volta in volta le soluzioni migliori per affrontare ciascun compito.
- dimensione cognitiva: fa riferimento alla capacità di cercare, usare e creare in modo critico le informazioni condivise in Rete, valutandone credibilità e affidabilità.
- dimensione etica e sociale: la prima fa riferimento alla capacità di gestire in

modo sicuro i propri dati personali e quelli altrui, e di usare le tecnologie digitali per scopi eticamente accettabili e nel rispetto degli altri. La seconda, invece, pone un po' più l'accento sulle pratiche sociali e quindi sullo sviluppo di particolari abilità socio comunicative e partecipative per maturare una maggiore consapevolezza sui nostri doveri nei riguardi di coloro con cui comunichiamo online.

Dalla integrazione di queste tre principali dimensioni emerge un concetto di competenza digitale che si basa sulla capacità di comprendere e sfruttare l'effettivo potenziale delle tecnologie in un'ottica sia di conoscenza ma anche di promozione della partecipazione e dell'inclusione: il rapporto con le tecnologie digitali allora diventa vincolante a un loro utilizzo consapevole, critico e creativo.

La formazione del curricolo digitale deve tener conto di quanto disposto dall'art. 5 della legge 20 agosto 2019 n. 92 (Introduzione dell'insegnamento scolastico dell'educazione civica) interamente dedicato alla cittadinanza digitale, intesa come capacità di un individuo di avvalersi consapevolmente e responsabilmente dei mezzi di comunicazione virtuali, dal Piano Scuola Digitale (PNSD), in particolar modo il paragrafo 4.2 su "Competenze e contenuti", dal DIGCOMP (quadro di riferimento per le competenze digitali del cittadino) e dalla sopra citata Raccomandazione del Consiglio europeo relativa alle competenze chiave per l'apprendimento permanente del 2018 (documento in cui vengono specificate le conoscenze, le abilità e gli atteggiamenti essenziali legati a tale competenza).

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 e del personale che opera nella scuola è un importante elemento di qualità nel servizio scolastico; essa rappresenta una leva strategica per lo sviluppo culturale dell'istituzione scolastica, per il necessario sostegno agli obiettivi di

cambiamento e per un'efficace politica delle risorse umane. Il Piano di formazione del personale docente recepisce le necessità emerse dal Rapporto di Autovalutazione (RAV) e dal Piano di Miglioramento (PDM) e le proposte indicate nel Piano Nazionale Scuola Digitale (PNSD). Il percorso della formazione specifica dei docenti sull'utilizzo delle TIC nella didattica deve diventare un processo permanente che prevede anche momenti di autoaggiornamento.

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.

La scuola invita, inoltre, tutti i docenti a effettuare la formazione sul sito Generazioni Connesse registrandosi e utilizzando il codice fornito dal referente per l'abbinamento alla scuola.

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.

Allo scopo di mantenere viva l'attenzione delle famiglie su tali temi, verranno inoltre valorizzate le opportunità di incontro e formazione per le famiglie sui temi oggetto della policy, offerte dal territorio, selezionando iniziative significative promosse da Enti e/o Associazioni di comprovata affidabilità.
Saranno favoriti momenti di confronto e di discussione tra studenti anche sulle dinamiche che potrebbero instaurarsi fra i pari mediante l'uso di smartphone, chatline e attraverso i social network più diffusi, con particolare riferimento alla prevenzione del cyberbullismo. E' stata attuata anche la possibilità di segnalare episodi di bullismo o cyberbullismo, attraverso uno spazio fisico dedicato (cassetta all'ingresso della segreteria alunni). Nell'Istituto è inoltre attivo lo sportello d'ascolto di consulenza psicologica e lo sportello per la gestione dei conflitti e la promozione della Cultura Riparativa con l'obiettivo di sostenere gli studenti in difficoltà, anche in merito a queste tematiche specifiche.

Nell'area dedicata sul sito, verrà data visibilità al portale del Garante della privacy, dove anche studenti minorenni possono segnalare e richiedere la rimozione di contenuti indesiderati che li riguardino (https://www.garanteprivacy.it/cyberbullismo), e del Comitato Regionale per le Comunicazioni (Co.re.Com.) della Regione Lombardia (https://www.corecomlombardia.it/wps/portal/site/comitato-regionale-comunicazioni/infopoint-web-reputation), dove è possibile prendere contatto per risolvere situazioni di diffamazione nella rete. In aggiunta, si segnalano un'applicazione della Polizia Postale per la segnalazione dei casi (App YouPol), la helpline di Generazioni Connesse (Tel. 1.96.96) e la chat del Telefono Azzurro, per una consulenza immediata (http://www.azzurro.it/chat/).

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2023/2024)

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

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

- Organizzare e promuovere per il corpo docente e per gli studenti incontri formativi sull’utilizzo consapevole e l’integrazione delle TIC nella didattica.

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 nostra scuola è impegnata in prima persona nella tutela della privacy. Le finalità e le modalità con cui l'Istituto raccoglie e tratta i dati personali, quali categorie di dati sono oggetto di trattamento, quali sono i diritti dell'Utente e come possono essere esercitati sono disponibili in un'area dedicata nel sito della scuola (https://www.cossali.edu.it/index.php/privacy).

Particolare attenzione è data nei confronti degli studenti quando questi sono minorenni, in ottemperanza all'articolo 8 della Carta dei diritti fondamentali dell'Unione europea tutelato dal regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, recepito dal nostro ordinamento dal D.Lgs. 10 agosto 2018 n. 101, entrato in vigore lo scorso 19 settembre 2018.

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'edificio scolastico dispone di una propria infrastruttura di rete, sia cablata sia wireless, che copre tutti gli spazi didattici e amministrativi dell'Istituto.
La rete della segreteria è dotata di server dedicato, utilizzato sia per il controllo e autorizzazione degli accessi del personale amministrativo sia per la gestione di tutte le applicazioni e dati, indispensabili per il normale lavoro di gestione della stessa.
Il Dirigente Scolastico, il Direttore dei Servizi Generali e Amministrativi ed il personale degli uffici della segreteria sono profilati con account personalizzati e accedono ai servizi tramite procedura di autenticazione personale che prevede l'utilizzo di password aventi caratteristiche adeguate e obbligo di sostituzione periodica.
La rete didattica è dotata di server dedicato che garantisce la connessione a tutte le classi dell'Istituto, dotate di pc laptop e video proiettori interattivi o di digital board, oltre ad offrire la connessione a laboratori, biblioteca, aula magna ed altri spazi dedicati al normale svolgimento delle lezioni o di altre attività.
L'accesso alla rete è consentito a docenti, personale, tecnici e alunni, con privilegi user tramite procedura di autenticazione personale che prevede l'utilizzo di password aventi caratteristiche adeguate e obbligo di sostituzione periodica e per solo fini didattici.
Gli studenti accedono alla rete sotto il controllo dei docenti e degli assistenti tecnici durante le attività didattiche.
L'I.I.S. Cossali è dotato di due reti Wifi, gestite con sistema Ubiquiti UniFi, una dedicata al personale scolastico con accessi filtrati attraverso l'indirizzo MAC, l'altra riservata al personale esterno e, su richiesta del docente, agli studenti il cui accesso avviene attraverso il rilascio da parte dell'amministrazione di un voucher con scadenza temporale.
Tutte le reti dell'Istituto sono dotate di firewall virtuale e backup automatico dei dati su supporto esterno (NAS). Su tutti i dispositivi sono stati installati sistemi atti a rilevare la presenza e a bloccare l'esecuzione di malware e vengono aggiornati automaticamente. Il traffico viene bloccato da e verso url presenti nella blacklist implementata sul Firewall.

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.

Tra gli sturmenti di comunicazione esterna Il nostro Istituto utilizza soprattutto il sito web della scuola www.cossali.edu.it
Inoltre dispone di registro elettronico, una e-mail scolastica personalizzata, applicativi e piattaforme di lavoro collaborativo e condiviso, tra cui G Suite Enterprise for Education che facilita la comunicazione digitale attraverso le apps: Meet, Drive, Gmail, Classroom.
Il registro elettronico permette di gestire la comunicazione con le famiglie, le quali attraverso di esso possono visualizzare molte informazioni utili, interagendo con la scuola, su:

- andamento scolastico (assenze, argomenti lezioni e compiti, note disciplinari);
- risultati scolastici (voti, documenti di valutazione);
- udienze (prenotazioni colloqui individuali);
- eventi (agenda eventi);
- comunicazione varie (comunicazioni di classe, comunicazioni personali).

3.4 - Strumentazione personale

I dispositivi tecnologici sono parte integrante della vita personale di ciascuno, compresa quella degli/lle studenti/esse e dei docenti (oltre che di tutte le figure professionali che a vario titolo sono inseriti nel mondo della scuola), ed influenzano necessariamente anche la didattica e gli stili di apprendimento. Comprendere il loro utilizzo e le loro potenzialità innovative, diventa di cruciale importanza, anche considerando il quadro di indirizzo normativo esistente e le azioni programmatiche, fra queste il Progetto Generazioni Connesse e il più ampio PNSD.

La presente ***ePolicy*** contiene indicazioni, revisioni o eventuali integrazioni di Regolamenti già esistenti che disciplinano l'uso dei dispositivi personali in classe, a seconda dei vari usi, anche in considerazione dei dieci punti del Miur per l'uso dei

dispositivi mobili a scuola (BYOD, “Bring your own device”).

Risulta fondamentale per la comunità scolastica aprire un dialogo su questa tematica e riflettere sulle possibilità per l’Istituto di dotarsi di una regolamentazione condivisa e specifica che tratti tali aspetti, considerando aspetti positivi ed eventuali criticità nella e per la didattica.

Come stabilito dal DPR 24 giugno 1998, n. 249, modificato dal DPR 21 novembre 2007, n. 235 e ribadito dalla Direttiva Ministeriale 15/03/2007, è vietato l’utilizzo dei telefonini all’interno della scuola durante le lezioni, salvo necessità didattiche e su disposizione dell'insegnante come previsto nel Regolamento di Istituto.

Il docente che rileva un uso non autorizzato del cellulare, lo ritirerà e lo depositerà in Dirigenza; il Dirigente Scolastico o un suo delegato lo riconsegnerà ai genitori dell’alunno/a minorenne. Se l’alunno è recidivo il Consiglio di Classe adotterà provvedimenti secondo la normativa vigente.

Gli studenti, inoltre, non possono accedere alla Rete attraverso i dispositivi della scuola se non previa autorizzazione dell’insegnante presente in aula e comunque solo per le attività didattiche.

Ai docenti è consentito l’utilizzo di dispositivi elettronici personali per fini didattici.

Il nostro piano d'azioni

AZIONI (da sviluppare nell’arco dell’anno scolastico 2023/2024).

- Organizzare eventi o attività volti a formare i docenti, gli studenti e le studentesse dell’Istituto sul tema delle tecnologie digitali e della protezione dei dati personali.
- Organizzare incontri sulla gestione della strumentazione ICT della e nella scuola.

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

- 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.

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.*

Prevenzione/Sensibilizzazione

I ragazzi nativi digitali usano normalmente le teconologie nella loro vita quotidiana. Essi non sempre colgono le implicazioni dei loro comportamenti, e tale fenomeno è tanto maggiore quanto è più forte il coinvolgimento emotivo nell'utilizzo dei nuovi

media. Le tecnologie digitali offrono da tempo la possibilità di ampliare la propria rete di amicizie in modo quasi smisurato: avere molti amici nella vita virtuale, o molti followers, è elemento di grande popolarità e di vanto con gli amici della vita reale. Non a caso gli adolescenti aggiungono tra le proprie cerchie, in particolare sui loro profili social, "amici di amici" e persone non conosciute, senza valutare attentamente a chi stanno dando accesso alle proprie informazioni, alle proprie foto, spesso ai luoghi che frequentano, a quello che viene chiamato "diario virtuale". La geo-localizzazione, inoltre, permette l'individuazione precisa del luogo in cui ci si trova. Tra le poche accortezze che molti ragazzi utilizzano per valutare l'affidabilità e la sicurezza di chi chiede loro di essere aggiunto tra gli amici, c'è quella di considerare il numero di amici in comune con la persona che aggiungono. Gli adolescenti spesso non usano l'autenticazione in due fattori, quindi i loro profili sono facili prede di accessi non autorizzati, e non hanno impostato nemmeno un alert in Google che permetta loro di vedere se c'è condivisione illecita di informazioni che li riguardino. Questo li espone a rischi notevoli: tra gli altri, quello di condividere con sconosciuti l'accesso al loro mondo online, e quindi a informazioni che potrebbero essere utilizzate in modo inaspettato e non sempre positivo. Aiutare i propri studenti a tutelarsi è un compito importante anche dell'insegnante, che contribuisce in questo modo alla loro tutela nella vita virtuale, con ripercussioni importanti nella vita reale.Tra i principali rischi, sia di carattere comportamentale che di matrice tecnica, ricordiamo:

- possibile esposizione a contenuti violenti e non adatti alla loro età;
- videogiochi diseducativi;
- pubblicità ingannevoli;
- accesso ad informazioni scorrette;
- virus informatici in grado di infettare computer e cellulari;
- rischio di molestie o maltrattamenti da coetanei (cyber- bullismo);
- scambio di materiale a sfondo sessuale (sexting);
- uso eccessivo di Internet/cellulare (dipendenza);
- adescamento on line (grooming).

È opportuno che i docenti sappiano cogliere ogni opportunità per riflettere insieme agli alunni su tali rischi. Fondamentale è monitorare costantemente le relazioni interne alla classe, onde individuare possibili situazioni di disagio ed intervenire tempestivamente per sostenere il singolo nelle situazioni di difficoltà personale e indirizzare il gruppo verso l'instaurazione di un clima positivo, di reciproca accettazione e rispetto, nelle situazioni di difficoltà socio-relazionale. Tale percorso interno potrà essere ulteriormente rinforzato dalla partecipazione a progetti e/o iniziative esterne coerenti con i temi sopra menzionati, cui la scuola porrà particolare attenzione, selezionando iniziative significative promosse da Enti e/o Associazioni di comprovata affidabilità.

Rilevazione

Laddove il docente colga possibili situazioni di disagio, connesse ad uno o più di uno tra i rischi elencati nel paragrafo «Prevenzione», dovrà informare il Dirigente

Scolastico ed il Team di emergenza per la prevenzione ed il contrasto al bullismo ed al cyberbullismo, verbalmente e/o attraverso la compilazione di una "scheda di segnalazione" (disponibile nell'area riservata del sito web istituzionale). La scheda di segnalazione potrà essere redatta dal docente sia sulla base di eventi osservati direttamente a scuola, sia su eventi particolari che gli sono stati confidati dall'alunno o comunicati da terzi.

Gestione dei casi

A seguito della segnalazione, il Dirigente Scolastico e e il Team per la prevenzione ed il contrasto al bullismo ed al cyberbullismo avranno cura di contattare il docente per un colloquio finalizzato a valutare la necessità di effettuare uno o più interventi di osservazione in classe e, successivamente, di pianificare adeguati interventi educativi e, ove necessario, di coinvolgere le famiglie per l'attivazione di un percorso comune e condiviso di sostegno al disagio. Le azioni poste in essere dalla scuola saranno dirette non solo a supportare le vittime, le famiglie e tutti coloro che sono stati spettatori attivi o passivi di quanto avvenuto, ma anche a realizzare interventi educativi rispetto a quanti abbiano messo in atto comportamenti lesivi, ove si tratti di soggetti interni all'Istituto. In situazioni di gravità maggiore si valuterà anche il coinvolgimento di attori esterni quali le forze dell'ordine e i servizi sociali.

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).

Nell' Istituto è stata individuato un Team di emergenza per situazioni di cyberbullismo e bullismo composto da un Referente e 6 docenti che hanno seguito il corso specifico di Piattaforma Elisa nell'a.s. 2021/2022.

Nell'ambito dei percorsi di Educazione Civica, si propongono unità (differenziate a seconda degli anni di corso) per informare gli studenti sulle modalità di diffusione e sui rischi correlati a questo fenomeno, nonché su comportamenti scorretti, di prevaricazione e discriminazione. Tali azioni di prevenzione e contrasto vengono condotte in sinergia con le associazioni presenti sul territorio e con le Forze dell'Ordine.

A supporto dei soggetti coinvolti sono previste azioni specifiche, quali incontri con lo psicologo; risoluzione del conflitto con incontro degli attori mediato da personale formato; applicazione di sanzioni disciplinari commisurate alla gravità degli atti compiuti finalizzate alla rieducazione, come da Regolamento d'Istituto.

Compito della comunità scolastica è vigilare sugli studenti, identificare vittime e prepotenti in divenire e intervenire sul gruppo classe con la collaborazione dei genitori. È infatti importante analizzare le relazioni sociali e l'ambiente in cui un fenomeno di cyberbullismo si verifica, per attuare un intervento mirato con la collaborazione del team docenti della classe, dello psicologo e dei mediatori.

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.

Prevenire e/o contrastare: per riuscire a far emergere l' "hate speech" si propongono annualmente, in diversi contesti (Progetto accoglienza, Star bene a scuola…) una serie di attività che mirano all’inclusione della diversità ed al rispetto con la creazione di un ambiente che favorisca la relazione tra pari, così come percorsi di Educazione Civica sulla salvaguardia dei diritti dell'uomo e del fanciullo.

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 nel suo ruolo educativo fornisce informazioni, attraverso il percorso di

Educazione civica, sulle varie tipologie di gioco on line e attua una prevenzione attraverso l'informazione e l'educazione dell'alunno all'uso consapevole di tutte le attività di gioco intese come momento di serenità e svago.

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.

A livello preventivo, l'Istituto attiverà percorsi di formazione rivolti agli studenti e ai docenti per approfondire i rischi e le conseguenze di episodi di sexting. E' importante offrire spunti per avviare il dialogo in classe con gli studenti, partendo da storie accadute o da fatti di cronaca da commentare per riflettere sui punti salienti:

- consapevolezza del proprio valore e della propria immagine;
- importanza dell' agire quanto prima, parlandone con una figura adulta;
- rispetto e responsabilità;
- forme sanzionatorie di natura rieducativa e di tutela.

Il docente che viene a conoscenza di un episodio di sexting, è tenuto a notificare il fatto al Team antibullismo e al Dirigente Scolastico, che provvederà con la segnalazione all'autorità giudiziaria.

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.

Sensibilizzare per contrastare tale fenomeno, capire inoltre il giovane e anticipare culturalmente il fenomeno. Il miglior modo per prevenire casi di adescamento online è accompagnare ragazze e ragazzi in un percorso di educazione (anche digitale) all'affettività e alla sessualità. Ciò aiuterebbe a renderli più sicuri emotivamente. È importante, inoltre, che ragazzi e ragazze sappiano a chi rivolgersi. Gli adulti coinvolti, genitori e docenti, devono essere un punto di riferimento per il minore che va compreso e ascoltato. Affinché ciò avvenga è necessario tenere sempre aperto un canale di comunicazione con loro sui temi dell'affettività, del digitale e della sessualità. Fondamentale, inoltre, è portare avanti un percorso di educazione digitale che comprenda lo sviluppo anche di capacità quali la protezione della propria privacy e la gestione dell'immagine e dell'identità online, la capacità di gestire adeguatamente le proprie relazioni online.

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 pedopornografia è un reato perseguibile d'ufficio e, come tale, se la realtà scolastica ne viene a conoscenza deve effettuare la denuncia all'autorità giudiziaria competente e garantire all'alunno, vittima di reato, il supporto psicologico. In particolare il personale docente e in generale il personale scolastico, in presenza di reati perseguibili di ufficio, deve riferire al dirigente scolastico la notizia di reato di cui è venuto a conoscenza nell'esercizio delle sue funzioni. Spetterà poi al Drigente scolastico l'obbligo di denunciare la notizia di reato all'autorità giudiziaria competente.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2023/2024).

- Organizzare un incontro informativo per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti agli/lle studenti/studentesse e ai docenti.
- Promuovere incontri per studenti e studentesse dedicati alla cittadinanza digitale come previsto dal paino di Educazione Civica dell'istituto.
- Organizzare un incontro per la promozione del rispetto della diversità, all'interno del progetto accoglienza per le classi prime, nel rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc..

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

- Organizzare un incontro informativo per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti agli/lle studenti/studentesse e ai docenti.
- Promuovere incontri per studenti e studentesse dedicati alla cittadinanza digitale come previsto dal paino di Educazione Civica dell'istituto.
- Organizzare un incontro per la promozione del rispetto della diversità, all'interno del progetto accoglienza per le classi prime, nel rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc..
- Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/lle studenti/studentesse.

Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

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

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

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

Nelle procedure:

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

Inoltre, la scuola **individua le figure che costituiranno un team** preposto alla gestione della segnalazione (gestione interna alla scuola, invio ai soggetti competenti).

Nell'affrontare i casi prevediamo la **collaborazione con altre figure, enti, istituzioni e servizi presenti sul territorio** (che verranno richiamati più avanti), qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.

Tali procedure sono comunicate e condivise con l'intera comunità scolastica.

Questo risulta importante sia per facilitare l'emersione di situazioni a rischio, e la conseguente presa in carico e gestione, sia per dare un messaggio chiaro a studenti e

studentesse, alle famiglie e a tutti coloro che vivono la scuola che la stessa è un luogo sicuro, attento al benessere di chi lo vive, in cui le problematiche non vengono ignorate ma gestite con una mobilitazione attenta di tutta la comunità.

La condivisione avverrà attraverso assemblee scolastiche che coinvolgono i genitori, gli studenti e le studentesse e il personale della scuola, con l'utilizzo di locandine da affiggere a scuola, attraverso news nel sito della scuola e durante i collegi docenti e attraverso tutti i canali maggiormente utili ad un'efficace comunicazione.

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

- **Cyberbullismo**: è necessario capire se si tratta effettivamente di cyberbullismo o di altra problematica. Oltre al contesto, vanno considerate le modalità attraverso le quali il comportamento si manifesta (alla presenza di un "pubblico"? Tra coetanei? In modo ripetuto e intenzionale? C'è un danno percepito alla vittima? etc.). È necessario poi valutare l'eventuale stato di disagio vissuto dagli/lle studenti/esse coinvolti/e (e quindi valutare se rivolgersi ad un servizio deputato ad offrire un supporto psicologico e/o di mediazione).
- **Adescamento online**: se si sospetta un caso di adescamento online è opportuno, innanzitutto, fare attenzione a non cancellare eventuali prove da smartphone, tablet e computer utilizzati dalla persona minorenne e inoltre è importante non sostituirsi al bambino/a e/o adolescente, evitando, quindi, di rispondere all'adescatore al suo posto). È fondamentale valutare il benessere psicofisico dei minori e il rischio che corrono. Vi ricordiamo che l'attuale normativa prevede che la persona coinvolta in qualità di vittima o testimone in alcune tipologie di reati, tra cui il grooming, debba essere ascoltata in sede di raccolta di informazioni con l'ausilio di una persona esperta in psicologia o psichiatria infantile.
- **Sexting**: nel caso in cui immagini e/o video, anche prodotte autonomamente da persone minorenni, sfuggano al loro controllo e vengano diffuse senza il loro consenso è opportuno adottare sistemi di segnalazione con l'obiettivo primario di tutelare il minore e ottenere la rimozione del materiale, per quanto possibile, se online e il blocco della sua diffusione via dispositivi mobili.

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

Vi suggeriamo, inoltre, i seguenti servizi:

- Servizio di Helpline 19696 e Chat di Telefono Azzurro per supporto ed emergenze;

- Clicca e segnala di Telefono Azzurro e STOP-IT di Save the Children Italia per

segnalare la presenza di materiale pedopornografico online.

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.

5.3. - Gli attori sul territorio

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

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

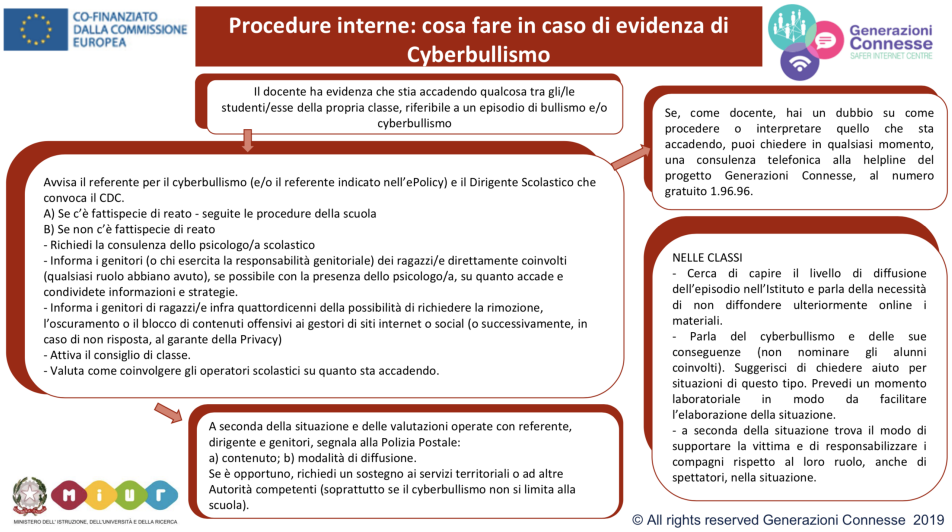
A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all'utilizzo di Internet può presentare.

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

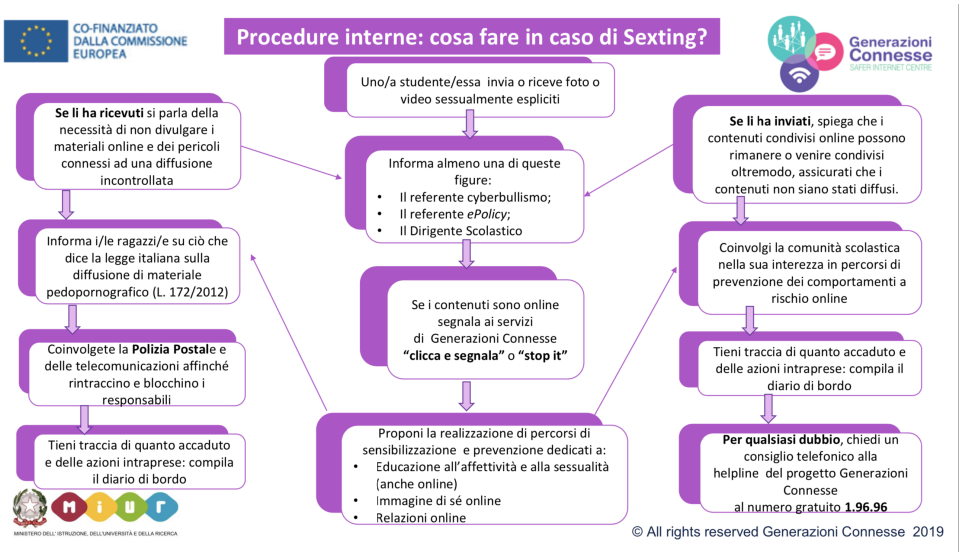
- **Tribunale per i Minorenni**: segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

5.4. - Allegati con le procedure

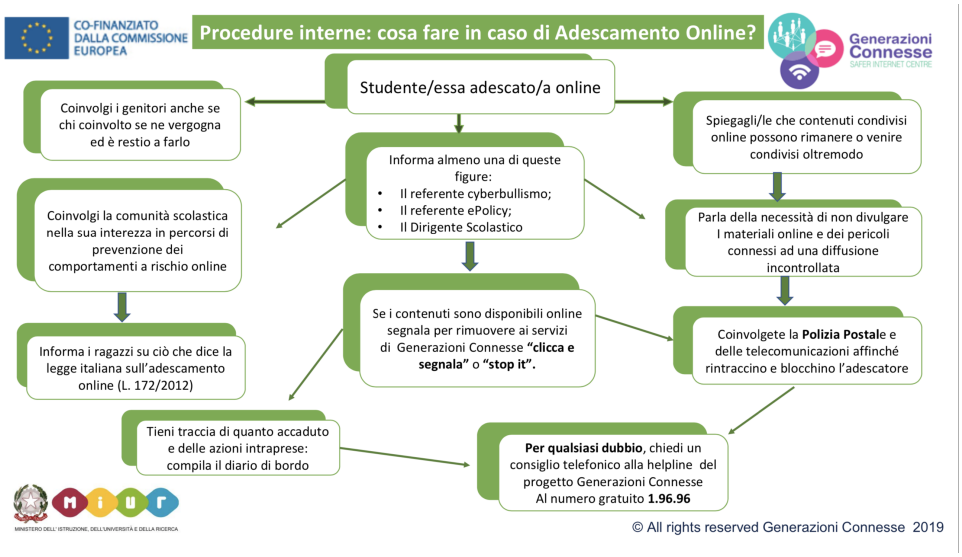
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



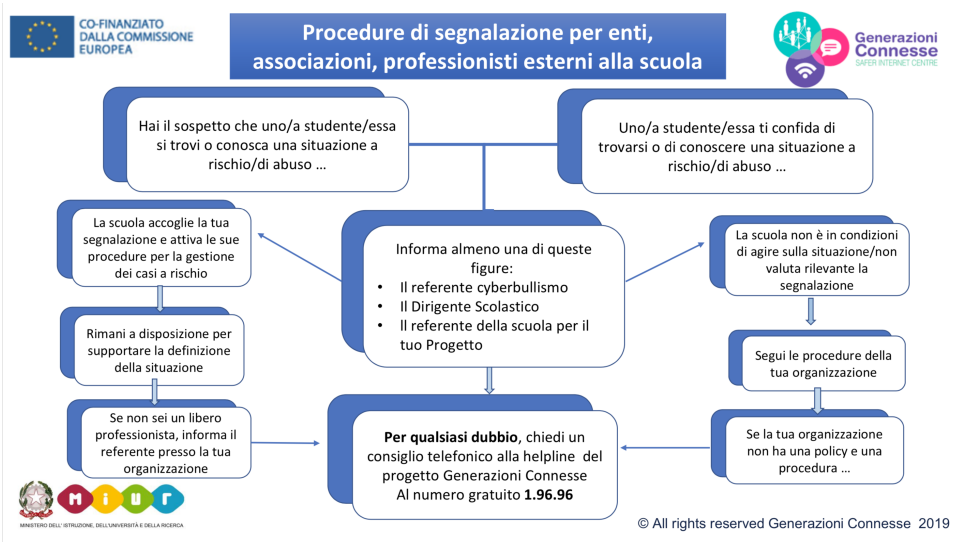
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



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



Altri allegati

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

Il nostro piano d'azioni

AZIONI DA INTRAPRENDERE IN BASE AL LIVELLO DI RISCHIO:
CODICE VERDE: LIVELLO DI RISCHIO BASSO
AZIONI: Situazione da monitorare con interventi preventivi nella classe.
CODICE GIALLO: LIVELLO DI RISCHIO MEDIO
AZIONI: interventi indicati e strutturati a scuola e in sequenza e coinvolgimento della rete se non ci sono risultati.
CODICE ROSSO: LIVELLO DI RISCHIO ALTO
AZIONI: Interventi di emergenza con supporto della rete.