



ISTITUTO COMPRENSIVO "MARIA GRAZIA CUTULI" - CROTONE
Prot. 0011377 del 16/12/2021
04 (Uscita)



Documento di ePolicy

KRIC81000G

I.C. "M. G. CUTULI" CROTONE

VIA BOCCIONI 1 - 88900 - CROTONE - CROTONE (KR)

ANNAMARIA MALTESE

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 curriculum**

1. Curriculum 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'I.C. "M.G. Cutuli da molti anni ha dato molto spazio all'Educazione alla Legalità nei suoi diversi aspetti inserendo nel PTOF anche il PNSD e corsi di aggiornamento e di formazioni sull'educazione digitale.

Molti gli incontri svolti tra gli alunni con esperti del settore tra cui la collaborazione con il Tribunale per i Minorenni di Catanzaro, con l'Arma dei Carabinieri, con la Polizia di Stato, con la Polizia Postale, con Psicologi, con Associazioni.

Inoltre, l'Istituto " M.G. Cutuli" è dotato di uno Sportello d'Ascolto con figure altamente qualificate, il team antibullismo, il team digitale. Da evidenziare che a prescindere dal ruolo specifico che ricopre ogni insegnante c'è sempre la massima collaborazione tra la componente docente, le famiglie e tutti gli attori esterni per favorire la formazione armonica della personalità degli alunni e rendere possibile un'adeguata integrazione sociale. Tale integrazione avviene soprattutto attraverso internet e i social network. I ragazzi, " nativi digitali", comunicano, giocano, interagiscono, studiano attraverso tecnologie multimediali che se usate in modo non responsabile, li espongono a grossi rischi di cui nemmeno loro sono consapevoli.

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.

La Policy di e-safety è un documento , autoprodotta dalla scuola, attraverso il quale si esplicitano i parametri di sicurezza digitale, le norme comportamentali e le procedure per l'utilizzo delle TIC in ambiente scolastico, nonché le misure di prevenzione per la rilevazione e la gestione delle problematiche connesse ad un uso improprio di tali tecnologie.

In sintesi il documento programmatico di E-Policy descrive:

- Il proprio approccio alle tematiche legate alle competenze digitali, alla sicurezza on line e ad un uso positivo delle tecnologie digitali nella didattica;
- Le norme comportamentali e le procedure per l'utilizzo delle Tecnologie dell'Informazione e della Comunicazione (ICT) in ambiente scolastico;
- Le misure per la prevenzione riguardo al cyberbullismo, alla cybersecurity e rispetto delle norme su privacy, copyright;
- Le misure per la rilevazione e gestione delle problematiche connesse ad un uso

non corretto delle tecnologie digitali.

Il documento vuole essere una base comune dell'azione didattico-educativa per il prossimo anno scolastico da estendere e fare conoscere a tutte le classi e alle famiglie, con un coinvolgimento di esperti ed associazioni che si occupano della materia per affrontare insieme nuove sfide-opportunità in questo ambito.

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.

Tutta la Comunità Scolastica è tenuta al rispetto delle norme contenute nel presente documento e si impegna ad un uso responsabile delle TIC, al fine di salvaguardare la sicurezza e i diritti di tutti i Cittadini digitali (ovvero tutti coloro che si connettono ad Internet attraverso dispositivi multimediali, in ambiente scolastico ed extrascolastico).

Il personale scolastico è tenuto a vigilare, nei limiti delle proprie competenze e possibilità, affinché il presente Regolamento sia rispettato e a segnalare le infrazioni secondo le procedure illustrate nel presente documento.

Studenti e genitori possono segnalare al personale scolastico eventuali infrazioni di cui sono venuti a conoscenza o situazioni di disagio che li vedano direttamente coinvolti in qualità di vittime.

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

Nel promuovere l'uso consentito delle tecnologie e di internet, il ruolo del Dirigente Scolastico è quello di:

- Garantire la tutela degli aspetti legali riguardanti la privacy e la tutela dell'immagine di tutti i membri della comunità scolastica;
- Garantire l'esistenza di un sistema di monitoraggio e il controllo interno alla sicurezza on line;
- Dover informare tempestivamente, qualora venga a conoscenza di atti di cyberbullismo, che non si configurino come reati, i genitori dei minori coinvolti.

REFERENTE CYBERBULLISMO D'ISTITUTO

Il ruolo del Referente per il Bullismo e Cyberbullismo include i seguenti compiti:

- Coordina iniziative di prevenzione e contrasto del cyberbullismo messe in atto dalla scuola, anche avvalendosi della collaborazione delle Forze di Polizia, nonché delle associazioni e dei centri di aggregazione giovanile presenti nel territorio;
- Svolge un importante compito di supporto al Dirigente, nonché all'istituzione scolastica per la revisione/stesura di Regolamenti, atti e documenti (PTOF, PDM ,modello di e-policy d'Istituto);
- Segnala tempestivamente situazioni di rischio on line o casi di bullismo e cyberbullismo;
- Collabora in team con altre figure scolastiche (Animatore digitale, Team antibullismo, Team per l'Innovazione, Referente Sportello d'Ascolto, Referente Bes/Inclusione, Referente per la Dispersione);
- Promuove la conoscenza e la consapevolezza riguardo al bullismo e al cyberbullismo, attraverso progetti d'Istituto che coinvolgano genitori, studenti e personale scolastico;
- Supporta i Consigli di Classe e i Coordinatori,
- Raccoglie e diffonde buone pratiche educative, organizzative e azioni di monitoraggio, anche attraverso la periodica somministrazione di questionari
- Facilita la formazione e la consulenza di tutto il personale scolastico.

ANIMATORE DIGITALE E TEAM DELL'INNOVAZIONE

Il ruolo dell'Animatore Digitale, coadiuvato dal Team per l'Innovazione, include i seguenti compiti:

- Pubblicare il documento di E-Policy sul sito della scuola;
- Stimolare la formazione interna all'istituzione negli ambiti di sviluppo della "scuola digitale", fornire consulenza ed informazioni al personale in relazione ai rischi on line e alle misure di prevenzione e gestione degli stessi;
- Monitorare e rilevare le problematiche emergenti relative all'utilizzo sicuro delle TIC e di internet a scuola;
- Individuare soluzioni tecnologiche innovative e sostenibili da diffondere nella scuola;
- Assicurare che gli utenti possano accedere alla Rete della scuola solo tramite password indicate dalla stessa scuola;
- Curare la manutenzione e lo sviluppo del sito web d'Istituto per scopi istituzionali consentiti.

DIRETTORE DEI SERVIZI GENERALI E AMMINISTRATIVI

Il ruolo del DSGA include i seguenti compiti:

- Assicurare, nei limiti delle risorse finanziarie disponibili, gli interventi di manutenzione necessari ad evitare un cattivo funzionamento della dotazione tecnologica dell'Istituto, controllando al contempo che le norme di sicurezza

vengano rispettate.

DOCENTI

Il ruolo del personale docente e di ogni figura educativa che lo affianca include i seguenti compiti:

- Provvedere alla propria formazione/aggiornamento sull'utilizzo del digitale, con particolare riferimento alla dimensione etica (tutela della privacy, rispetto dell'immagine degli altri: lotta al cyberbullismo);
- Promuovere la cultura dell'uso consapevole e corretto delle nuove tecnologie e della Rete, del rispetto della privacy e della dignità di ciascuno;
- Prevenire e intercettare situazioni legate ad un uso scorretto delle nuove tecnologie;
- Applicare la e-policy
- Collaborare con il Dirigente Scolastico, il Referente d'Istituto per il cyberbullismo, l'Animatore digitale e il Team per l'Innovazione, il Team antibullismo.

PERSONALE ATA

IL personale ATA si impegna a:

- Collaborare con Il Dirigente Scolastico, il DSGA e i docenti nella prevenzione ed intercettazione di situazioni legate ad un uso scorretto delle nuove tecnologie;
- Leggere e rispettare il presente documento di E-Safety Policy

GENITORI

I genitori svolgono un ruolo cruciale nel garantire che i minori comprendano la necessità di utilizzare in modo sicuro, consapevole ed appropriato dispositivi digitali. Per tale scopo è necessario che essi:

- Leggano e comprendano l'importanza del documento e-policy;
- Contribuiscano, in sinergia con il personale scolastico, alla sensibilizzazione dei propri figli sul tema della sicurezza in Rete;
- Sostengano l'Istituzione scolastica nel promuovere buone pratiche di e-safety;
- Consultino sul sito la Legge 29 maggio 2017 n. 71 recante "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo";
- Comunicino ai docenti difficoltà o disagi espressi dai propri figli nell'uso dei dispositivi digitali
- Approfondiscano e concordino con i docenti eventuali interventi con la psicologa dello Sportello d'Ascolto

Agiscano in modo concorde con la scuola per la prevenzione dei rischi e l'attuazione

delle procedure previste in caso di violazione delle regole stabilite

ALUNNI

Il ruolo degli alunni prevede i seguenti compiti:

- Leggere, comprendere ed accettare il documento di E-Safety Policy;
- Avere consapevolezza delle situazioni di rischio legate alla Rete;
- Partecipare ad incontri con le Forze dell'Ordine sulle opportunità e i rischi di un uso scorretto dei dispositivi digitali;
- Conoscere la politica della scuola sull'uso dei dispositivi mobili e sull'uso delle immagini;
- Comprendere l'importanza di adottare buone pratiche di sicurezza on line;
- Adottare condotte rispettose degli altri anche durante la comunicazione in rete;
- Essere consapevoli del significato e della gravità di atti di cyberbullismo, a tutela della propria ed altrui incolumità;
- Assumersi la responsabilità di un eventuale utilizzo sbagliato delle tecnologie.

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).

da compilare con le indicazioni contenute nella lezione

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/le 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 documento sarà reso noto al personale/alunni/comunità scolastica nei seguenti modi:

- sul sito della scuola, una volta approvato in modo definitivo
- bacheca dei plessi
- sul registro elettronico

Si solleciteranno i genitori a visionare il documento anche attraverso comunicazione scritta sul diario scolastico. Inoltre, l'e-policy sarà integrato al Patto di Corresponsabilità e al Regolamento d'Istituto.

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.

Le sanzioni avranno carattere educativo/riabilitativo, con il coinvolgimento delle famiglie.

Nell'ottica di una didattica sempre più digitale, si garantisce agli studenti l'accesso a materiale e ambienti appropriati. Nonostante tutto, risulta difficoltoso evitare in assoluto che essi trovino materiale "improprio" durante la navigazione a scuola, pertanto l'Istituzione scolastica non può assumersi alcuna responsabilità. Qualsiasi sospetto, rischio, uso improprio, violazione va segnalato immediatamente al Dirigente che, eventualmente, riferisce direttamente alle autorità di competenza (v. protocollo dei rischi rilevati). Il personale, gli studenti e gli altri componenti della comunità scolastica sono informati sulle infrazioni previste e le eventuali sanzioni.

1.6 - Integrazione dell'ePolicy con Regolamenti esistenti

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

La e-policy, una volta approvata, diventa parte integrante di tutti i regolamenti vigenti nell'Istituto, in particolare del Regolamento d'Istituto e P.U.A. (Politica di Uso Accettabile), costituendo la sezione relativa all'uso delle nuove tecnologie, dei nuovi ambienti di apprendimento e delle metodologie didattiche offerti dall'Istituto.

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'E-policy, della validità triennale, può essere aggiornata annualmente e/o quando si verificano cambiamenti significativi in riferimento all'uso delle tecnologie digitali all'interno della scuola.

Il monitoraggio dell'implementazione della Policy può avvenire:

- Alla fine di ogni anno scolastico, sulla base dei casi problematici riscontrati e della loro gestione;
- All'inizio di ogni anno scolastico, contestualmente alla revisione del PTOF, a seguito di verifica atta a constatare l'insorgenza di nuove necessità.

Il nostro piano d'azioni

Azioni da svolgere nel triennio, a partire dall'anno scolastico 2021/2022:

- Organizzare uno o più eventi o attività volti a presentare il progetto alla comunità scolastica (Dirigente Scolastico, DSGA, docenti, ATA, alunni, genitori).
- Organizzare incontri con le Forze dell'Ordine, Tribunale per i Minorenni, esperti del settore rivolti a studenti, genitori e docenti

Capitolo 2 - Formazione e curriculum

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 curriculum digitale.

Il curriculum disciplinare del nostro Istituto prevede, tra gli obiettivi, l’acquisizione delle competenze digitali sviluppandole trasversalmente tra le varie discipline. Il raggiungimento di tali obiettivi si ottiene attraverso l’uso delle TIC, inserite nelle attività didattiche, un’alfabetizzazione informatica e digitale, atta a fornire gli strumenti per un uso consapevole, critico, autonomo e responsabile dei device digitali e, infine, una consapevolezza dei rischi della rete, grazie al supporto di esperti esterni.

L’Istituto sta provvedendo all’implementazione della dotazione digitale dei plessi, grazie alla partecipazione ai progetti PON, che consentiranno un diffuso ricorso alle nuove metodologie legate all’uso delle TIC e una maggiore accessibilità in termini di connessione.

La convenzione con AICA, inoltre, consentirà di attivare corsi indirizzati alla comunità scolastica, finalizzati all’ottenimento della certificazione ECDL.

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

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

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

Il Piano Triennale dell'Offerta Formativa prevede la formazione dei docenti attraverso corsi organizzati dall'Istituzione, dalla Scuola Polo, dall'USR, dal MIUR o altri enti riconosciuti finalizzati all'accrescimento delle competenze digitali di base. Allo stesso modo, per l'animatore digitale e i docenti del team digitale sono previsti corsi di formazione e/o aggiornamento, spendibili all'interno dell'Istituto.

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 formazione specifica dei docenti sull'utilizzo consapevole e sicuro di Internet prevede corsi di autoaggiornamento, individuali o collettivi per stare al passo dell'evoluzione delle tecnologie, di cui usufruiscono ormai quotidianamente e

sistematicamente gli studenti, in modo da poter fornire loro una guida e supporto.

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.

L'Istituto promuove iniziative per sensibilizzare le famiglie all'uso consapevole delle TIC e della rete e dei rischi ad essi connessi, attraverso favorire incontri tra le famiglie ed esperti (psicologi, forze dell'ordine). Attraverso il Patto di Corresponsabilità e incontri preliminari coi genitori, l'Istituto sottolinea il rischio derivante dall'uso di smartphone e dei social network diffusi tra i ragazzi. Sul sito dell'istituto saranno inseriti materiali per alunni, docenti e famiglie su tali rischi e sul fenomeno, ad essi collegato, del cyberbullismo. Sarà inoltre diffuso il Regolamento sull'utilizzo delle nuove tecnologie all'interno dell'Istituto.

Il nostro piano d'azioni

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

- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie

digitali.

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

AZIONI (da sviluppare nell'arco del triennio 2022-2025)

- 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.
- Organizzare incontri con esperti per i genitori sull'educazione alla cittadinanza digitale.

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

3.1 - Protezione dei dati personali

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

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

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

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

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

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

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

Tra le norme da seguire a tutela della privacy, i principali riferimenti riguardano:

- Divieto di condividere i propri contatti personali (salvo casi specifici ed eccezionali), privilegiando i canali istituzionali della scuola (telefono, email di istituto, Registro elettronico).
 - Al momento dell'iscrizione le famiglie dovranno firmare un'autorizzazione per consentire l'uso di immagini e video delle/dei minori per finalità strettamente connesse alla vita scolastica: ovviamente, la pubblicazione di fotografie o video da pubblicare sul sito, terranno conto dei consensi espressi dai genitori ad inizio anno scolastico.
 - Ogni iniziativa che preveda la trasmissione alla scuola di dati personali sarà accompagnata da un modulo di consenso informato da parte delle famiglie.
-

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.

Il servizio di assistenza tecnica provvederà alla revisione del sistema di filtraggio e all'installazione di adeguati sistemi anti virus, in modo da garantire una navigazione sicura ed efficace.

L'Istituto è fornito di rete wireless a cui si connettono la maggiorparte dei dispositivi, con l'eccezione dei dispositivi in uso presso l'ufficio di segreteria e i laboratori informatici, dove è prevista una connessione via cavo.

Attraverso il ricorso a fondi provenienti da PON si sta provvedendo al miglioramento dell'efficienza delle reti wireless, con il passaggio alla fibra ottica, per l'implementazione della rete. I dispositivi sono collegabili alla rete internet esclusivamente tramite password. Il personale docente di ogni plesso, è a conoscenza della password di accesso, così da poter connettere facilmente tutti i dispositivi necessari per lo svolgimento delle attività didattiche. Nell'ottica di un maggior sviluppo del "Byod" (ossia l'utilizzo di dispositivi elettronici personali durante le attività didattiche), soprattutto nella scuola Secondaria di Primo Grado, e nello specifico il corso ad Indirizzo Digitale, si è fornita la password d'accesso alla rete anche agli alunni.

3.3 - Strumenti di comunicazione online

Le tecnologie digitali sono in grado di ridefinire gli ambienti di apprendimento, supportando la comunicazione a scuola e facilitando un approccio sempre più collaborativo. L'uso degli strumenti di comunicazione online a scuola, al fianco di quelli più tradizionali, ha l'obiettivo di rendere lo scambio comunicativo maggiormente

interattivo e orizzontale. Tale uso segue obiettivi e regole precise correlati alle caratteristiche, funzionalità e potenzialità delle tecnologie digitali.

L'Istituto ha un unico indirizzo di posta elettronica, che fa capo al Dirigente Scolastico ed è utilizzato per le comunicazioni ufficiali. Il personale interno alla scuola (D.S., docenti, personale di segreteria) e i genitori hanno a disposizione la piattaforma di registro elettronico "Nuvola" per le comunicazioni interne.

L'Istituto è registrato sulla piattaforma Gsuite, che consente di usufruire di diverse applicazioni utili alla didattica, dalla creazione di classi virtuali, di riunioni virtuali, alla condivisione di file e la progettazione di attività online. Docenti e alunni dei tre ordini di grado hanno acquisito le credenziali per accedere alla piattaforma, per lo svolgimento di lezioni in DAD/DDI e per la condivisione di materiale di approfondimento; inoltre attraverso questo strumento, nell'attuale periodo di emergenza sanitaria, si svolgono gli incontri scuola-famiglia e gli incontri collegiali.

L'Istituto ha un proprio sito web (www.isitutocutulikr.edu.it) che rappresenta il punto di informazione primaria per gli esterni: oltre alle informazioni generali e di contatto, vi si trovano apposite sezioni dedicate a docenti, personale ATA e famiglie degli alunni con informazioni, circolari, modulistica, presentazione di attività e progetti. La scuola, al momento, non dispone di un blog. E' stato creato lo scorso anno un account ad un social network per consentire la partecipazione dell'Istituto ai Safer Internet Days nell'anno scolastico 2020/2021, ma le attività collegate a tale social sono state limitate esclusivamente a questo evento. si sta riflettendo sulla possibilità di crearne uno nel quale racchiudere interventi ed esperienze degli alunni.

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.

L'utilizzo delle TIC in ambito didattico è considerato dai docenti dell'Istituto un grande supporto alle attività, soprattutto per la possibilità di tener conto dei diversi stili di apprendimento degli alunni e la capacità di coinvolgimento e partecipazione attiva, efficace ed efficiente da parte di tutti gli studenti.

Gli alunni della scuola dell'infanzia e primaria non possono utilizzare dispositivi personali, la connessione e l'utilizzo di dispositivi in uso presso i laboratori informatici avvengono sotto la stretta supervisione dei docenti. Presso la scuola secondaria di primo grado, gli studenti non sono autorizzati ad utilizzare i propri dispositivi se non autorizzati dai docenti per fini didattici e sempre sotto la supervisione degli insegnanti. Fanno eccezione gli studenti del corso a indirizzo digitale, che seguendo una politica di BYOD, propria dell'indirizzo, rende necessario l'utilizzo di un dispositivo personale (smartphone, tablet, PC) durante le attività didattiche.

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

AZIONI (da sviluppare nell'arco del triennio 2022-2025).

Scegliere almeno 1 di queste azioni:

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli
- studenti e delle studentesse
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte dei docenti
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte del personale Tecnico Amministrativo e dagli ATA
- Organizzare uno o più eventi o attività volti a consultare i docenti dell'Istituto per redigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali.
- Organizzare 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 i genitori dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

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

4.1 - Sensibilizzazione e Prevenzione

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

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

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

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

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

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).

L'Istituto presenta all'interno del proprio Curricolo un progetto alla legalità, che affronta i temi legati al cyberbullismo attraverso una serie di incontri con specialisti del settore (psicologi, forze dell'ordine).

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.

Saranno previsti diversi incontri formativi per gli alunni con l'ausilio dei docenti e di specialisti esterni, volti a riconoscere, prevenire e contrastare il fenomeno dell'Hate Speech, educando contestualmente al rispetto per le diversità e la tolleranza.

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?

In considerazione dell'incalzante crescita del fenomeno, l'Istituto pone tra le sue priorità la prevenzione di problematiche legate alla dipendenza da Internet attraverso la promozione di incontri a cura dei docenti e di personale esterno (psicologi, polizia

postale ecc.). Tali incontri coinvolgeranno tutta la comunità scolastica e l'attivazione dello sportello d'ascolto offrirà un notevole supporto a docenti, alunni e famiglie.

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 medialti 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.

Da implementare con le indicazioni contenute nella lezione.

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.

Saranno organizzati momenti di formazione rivolti a docenti, familiari e alunni per

comprendere e prevenire tale fenomeno anche con l'ausilio di psicologi e polizia postale. Per gli alunni, considerata la delicata fascia di età, sarà necessario iniziare un percorso di educazione all'affettività

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](#).

Da implementare con le indicazioni contenute nella lezione.

Il nostro piano d'azioni

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

- ☐ 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 di formazione all'utilizzo sicuro e consapevole di Internet e delle tecnologie digitali integrando lo svolgimento della didattica e assicurando la partecipazione attiva degli studenti/studentesse.
- ☐ Promuovere incontri e laboratori per studenti e studentesse dedicati all'Educazione Civica Digitale.
- ☐ Organizzare uno o più incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/lle studenti/studentesse.

AZIONI (da sviluppare nell'arco del triennio 2022-2025).

- ☐ 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 genitori e ai docenti, con il coinvolgimento di esperti.

☐ Organizzare uno o più incontri di formazione all'utilizzo sicuro e consapevole di Internet e delle tecnologie digitali integrando lo svolgimento della didattica e assicurando la partecipazione attiva degli studenti/studentesse.

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

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

☐ Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/le studenti/studentesse.

☐ Organizzare uno o più eventi e/o dibattiti in momenti extra-scolastici, sui temi della diversità e sull'inclusione rivolti a genitori, studenti/studentesse e personale della scuola.

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/le 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](tel:19696).

L'Istituto mette a disposizione una scatola per la raccolta di segnalazioni anonime; è attivo lo sportello d'ascolto con professionisti. Sarà cura del docente referente per il Bullismo e Cyberbullismo coinvolgere tutti gli attori del caso specifico.

5.3. - Gli attori sul territorio

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

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

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

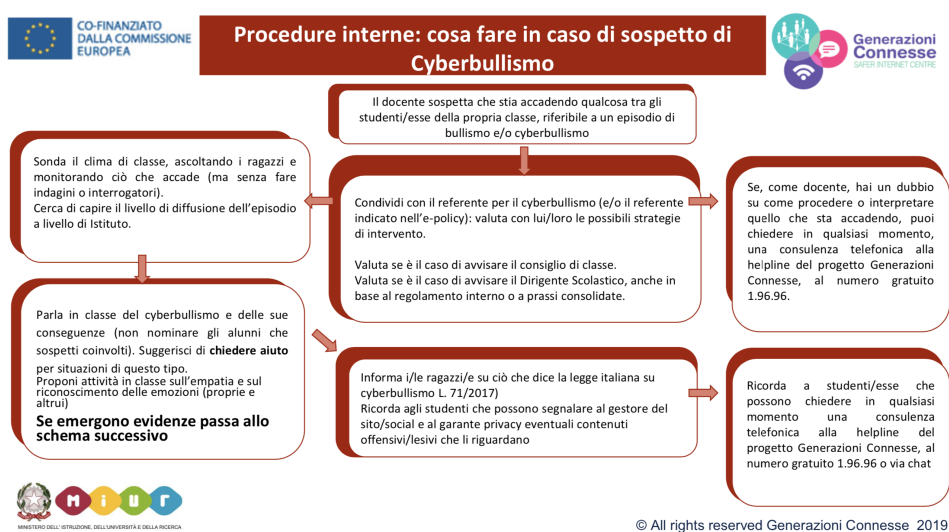
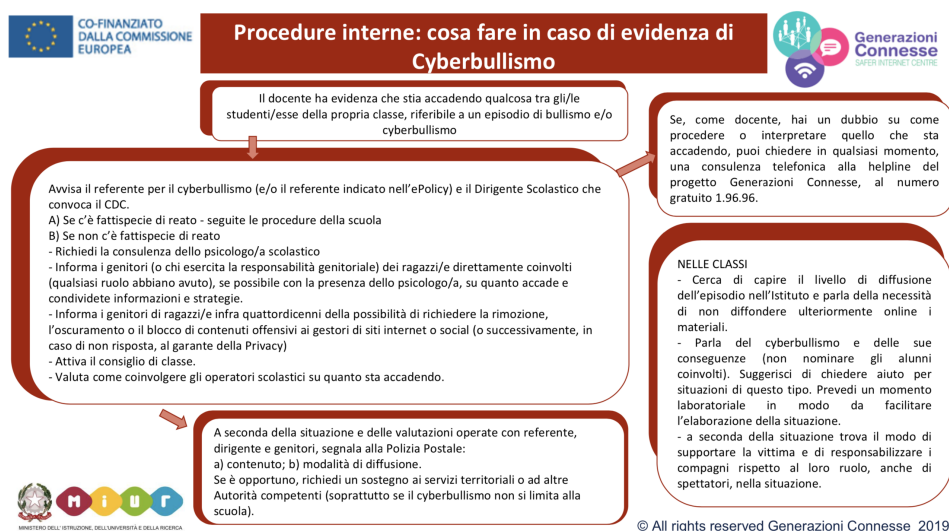
- **Comitato Regionale Unicef:** laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni):** svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare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

segnalano all'Autorità Giudiziaria e ai Servizi Sociali competenti; accolgono le segnalazioni di presunti abusi e forniscono informazioni sulle modalità di tutela e di esercizio dei diritti dei minori vittime. Segnalano alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.

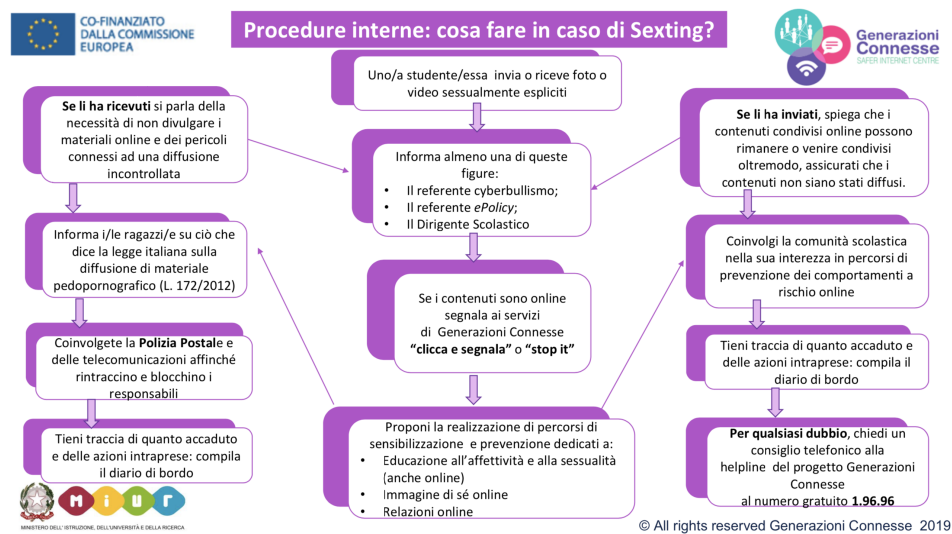
- **Tribunale per i Minorenni:** segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

5.4. - Allegati con le procedure

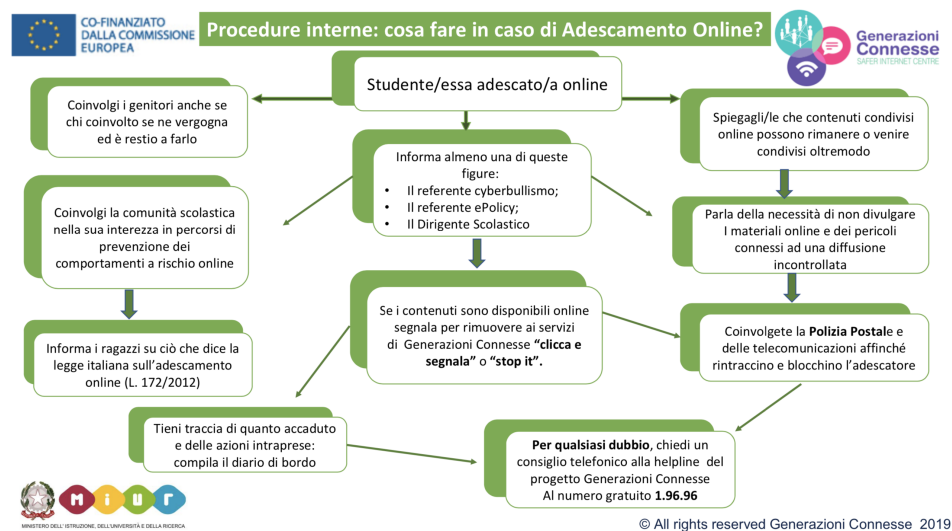
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



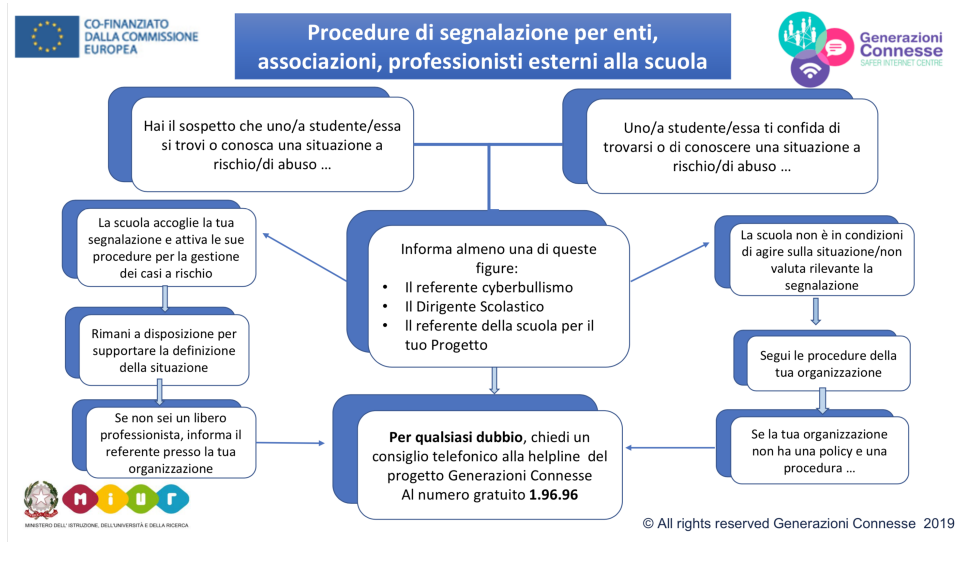
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



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



Altri allegati

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

Il nostro piano d'azioni

Non è prevista nessuna azione.

Il Dirigente Scolastico
Dott.ssa Annamaria Maltese
firmato digitalmente

