Documento di ePolicy

CSIC88800N

IC "EMILIO BIANCO" MONTALTO UFFUGO

VIA PAOLO BORSELLINOSNC - 87046 - MONTALTO UFFUGO - COSENZA (CS)

Gemma Faraco

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.

Questo documento elaborato, in collaborazione con il Safer Internet Centre, nell'ambito del Progetto "Generazioni Connesse" vuole coinvolgere tutte le componenti della Comunità scolastica: il personale della Scuola, gli alunni e le famiglie.

La presente e-Policy è stata redatta in conformità con le "Linee di orientamento per azioni di prevenzione e di contrasto al bullismo e cyberbullismo" emanate dal MIUR in collaborazione con il Safer Internet Center (SIC) per l'Italia, progetto co-finanziato dalla Commissione Europea nell'ambito del programma "Connecting Europe Facility" (CEF) - Telecom, con l'obiettivo di diffondere campagne di sensibilizzazione, promuovere azioni, risorse e servizi per un uso consapevole e responsabile delle tecnologie digitali e per la segnalazione delle problematiche connesse.

Il presente Documento è parte integrante del PTOF di Istituto e le azioni sottoscritte costituiscono indicazioni e buone prassi di azione e prevenzione in materia di bullismo e cyberbullismo.

1.2 - Ruoli e responsabilità

Affinché l'E-policy sia davvero uno strumento operativo efficace per la scuola e tutta la comunità educante è necessario che ognuno, secondo il proprio ruolo, s'impegni nell'attuazione e promozione di essa.

RUOLO	RESPONSABILITÀ

Il Dirigente Scolastico	● garantisce la sicurezza, anche online, di tutti i membri della comunità scolastica; ● promuove la cultura della sicurezza online e corsi di formazione specifici, d'accordo con il docente Referente per il bullismo e il Cyberbullismo; ● promuove la formazione di tutto il personale scolastico sull'uso positivo e responsabile delle tic, sulle potenzialità e i rischi della rete; ● dà attuazione al protocollo di e-Policy e ne promuove l'aggiornamento; ● fa parte del Team per l'Emergenza (insieme all'Animatore digitale, al Referente bullismo, allo psicologo individuato dall'Istituto) e del Team antibullismo per gestire e intervenire nei casi di gravi episodi di bullismo, cyberbullismo e uso improprio delle tecnologie digitali; ● intrattiene i rapporti con le agenzie competenti e le autorità locali; ● promuove il coordinamento tra le figure istituzionalmente preposte all'utilizzo delle TIC a scuola (Responsabile della Sicurezza, Amministratore di sistema e Animatore Digitale).
Il Referente bullismo e cyberbullismo	● coordina le iniziative di prevenzione e di contrasto del bullismo e del cyberbullismo all'interno dell'Istituto; ● fa parte del Team per l'Emergenza (insieme al Dirigente Scolastico, all'Animatore digitale, allo psicologo individuato dall'Istituto) e del Team antibullismo per gestire e intervenire nei casi di gravi episodi di bullismo, cyberbullismo e uso improprio delle tecnologie digitali; ● coordina la Commissione Bullismo della scuola, con il compito di proporre attività didattiche e iniziative volte a stimolare comportamenti responsabili, a sensibilizzare e a prevenire prevaricazioni e ogni forma di bullismo; ● può avvalersi delle forze dell'ordine e delle associazioni del territorio; ● coinvolge studenti, colleghi e genitori in progetti e percorsi formativi specifici;
L'Animatore digitale e il suo team	● supporta il personale scolastico da un punto di vista non solo tecnico-informatico, ma anche in riferimento ai temi della sicurezza online; ● può monitorare e rilevare le problematiche relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola; ● promuove percorsi di formazione interna all'Istituto negli ambiti di sviluppo del PNSD; ● può fare in modo che gli utenti autorizzati accedano alla Rete della scuola con apposita password e che i pc delle aule siano dotati di password; ● fa parte del Team per l'Emergenza e del Team antibullismo per gestire e intervenire nei casi di gravi episodi di bullismo, cyberbullismo e uso improprio delle tecnologie digitali;

I docenti	● educano gli alunni ad un uso responsabile della rete e delle TIC; ● promuovono l'uso delle tecnologie digitali nella didattica, accompagnando gli alunni nelle attività di apprendimento e nei laboratori che prevedono l'uso di dispositivi tecnologici; ● informano gli alunni sulle procedure da seguire per la segnalazione di atti di bullismo e cyberbullismo; ● si formano e autoformano sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di internet; ● hanno il dovere professionale di segnalare al Dirigente Scolastico qualunque problematica, violazione o abuso che coinvolga gli studenti; ● usano comportamenti sicuri, responsabili e professionali nell'uso della tecnologia;
Il personale Amministrativo,Tecnico e Ausiliario (ATA)	● usa comportamenti sicuri, responsabili e professionali nell'uso della tecnologia; ● è consapevoli dei problemi di sicurezza online connessi con l'uso di dispositivi multimediali; ● ha il dovere di segnalare qualsiasi sospetto abuso informatico alle figure di sistema, nonché di raccogliere verificare e valutare informazioni inerenti possibili casi di bullismo/cyberbullismo; ● può formarsi e auto-formarsi in tema di bullismo e cyberbullismo.
Gli studenti e le studentesse	● in relazione al grado di maturità e consapevolezza raggiunti, utilizzano le tecnologie digitali in coerenza con quanto richiesto dai docenti; ● conoscono le linee guida dell'E-safety Policy, il Regolamento d'Istituto (relativamente all'uso non corretto dei dispositivi tecnologici e in materia di bullismo/cyberbullismo) e il Patto di Corresponsabilità, che hanno sottoscritto; ● capiscono l'importanza di segnalare ad adulti di riferimento eventuali abusi o l'uso improprio della Rete e dei dispositivi digitali; ● imparano a tutelarsi online, a tutelare compagni/e e a rispettarli/e ● utilizzano i dispositivi tecnologici personali esclusivamente su autorizzazione del docente e solo per specifiche attività didattiche; ● possono farsi promotori delle buone pratiche apprese, anche attraverso possibili percorsi di peer education.
I genitori	● sono partecipi e attivi nelle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete; ● accettano e condividono l'e-Policy d'Istituto, il Regolamento d'Istituto e il Patto di Corresponsabilità; ● conoscono le linee di intervento della Scuola in relazione ai problemi rilevati ad un uso non responsabile o pericoloso delle tecnologie digitali o di internet; ● si relazionano in modo costruttivo con i docenti sulle linee educative che riguardano TIC e la Rete, monitorando i propri figli e segnalando eventuali problemi.

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, gli specialisti, i formatori e le associazioni esterne che entrano in relazione con la scuola sono tenuti a conformarsi alla politica della stessa riguardo all'uso consapevole della Rete e delle TIC, adottando e promuovendo comportamenti sicuri e proteggendo gli studenti durante le attività che si svolgono assieme. In coerenza con il percorso intrapreso viene predisposta un'informativa sintetica sull'e-Policy comprensiva delle "procedure di segnalazione" in caso di illecito e di episodi che mettano in pericolo studenti e studentesse. Le procedure di segnalazione contengono i riferimenti interni alla scuola cui rivolgersi in caso di necessità, come il Referente bullismo e il coordinatore della/e classe/i coinvolta/e nel progetto.

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.

All'inizio dell'anno scolastico, in occasione dell'illustrazione del Regolamento di Istituto agli alunni da parte dei docenti, verrà presentata la ePolicy dell'Istituto insieme ai regolamenti correlati e al Patto di Corresponsabilità. La ePolicy, redatta dal Gruppo di lavoro, nonchè dalla commissione bullismo/cyberbullismo e approvata dal collegio Docenti e dal Consiglio di Istituto, sarà inserita all'interno del PTOF.

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 potenziali infrazioni a carico degli alunni sono identificabili in: - uso di social network e blog per pubblicare, condividere o, in genere, postare commenti o giudizi offensivi della dignità altrui; - condivisione di dati personali che possano permettere l'identificazione; - produzione e/o pubblicazione di foto e immagini non autorizzate e/o compromettenti; - connessioni a siti non autorizzati. Gli interventi educativi previsti per gli alunni saranno rapportati all'età e al livello di sviluppo del discente. Un primo intervento viene attuato dal docente secondo le seguenti modalità: - richiamo verbale; - richiamo verbale con annotazione disciplinare sul registro e sul diario personale; - convocazione della famiglia.

Le potenziali infrazioni a carico del personale scolastico sono identificabili in: - utilizzo delle tecnologie e dei servizi della scuola, d'uso comune con gli alunni, non adeguate alle attività di insegnamento e al profilo professionale; - trattamento dei dati personali, comuni e sensibili degli alunni, non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi; - custodia non adeguata degli strumenti e degli accessi di cui possono approfittare terzi.

Il Dirigente scolastico può monitorare la modalità di utilizzo delle TIC da parte del personale scolastico servendosi di idonei strumenti di controllo che consentono di individuare e bloccare preventivamente eventuali anomalie, nel rispetto della privacy degli utenti. Il personale collabora con il Dirigente scolastico e fornisce ogni informazione utile per le valutazioni del caso e per l'avvio di procedimenti che possono avere carattere organizzativo-gestionale, disciplinare, amministrativo, penale, a seconda del tipo o della gravità delle infrazioni commesse.

Le procedure sono quelle previste dalla legge e dai contratti di lavoro.

1.6 - Integrazione dell'ePolicy con Regolamenti esistenti

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

Il presente documento si integra pienamente con gli obiettivi e i contenuti del PTOF e del Regolamento interno d'Istituto, che specificano il contesto di attuazione delle politiche della scuola per un uso efficace e consapevole delle tecnologie digitali.

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.

da compilare con le indicazioni contenute nella lezione

Il nostro piano d'azioni

Azioni poste in essere

Classi seconde Scuola Primaria - Progetto/Concorso “Amici di grembiule”, Progetto "CODE the NATURE"

Classi quarte scuola Primaria - Progetto di formazione/sperimentazione "Geronimo Stilton e i diritti dei bambini nell’ambiente digitale"

Classi quinte scuola primaria - Incontro con la Polizia di Stato per discutere dei pericoli del web. Partecipazione al Progetto/Concorso "Pretendiamo Legalità", proposto dalla Questura di Cosenza; Progetto "BenConnessi" (Fondo permanente per il contrasto del fenomeno del cyberbullismo” Legge n. 234 del 2021, articolo 1, comma 671. Decreto dipartimentale n. 513 del 26 aprile 2023)

Tutte le classi dell'Istituto - Partecipazione al Safer Internet Day con attività didattiche curricolari.

Classi prime e seconde Scuola Secondaria di primo grado - Progetto”il Bullo! No, grazie” - Progetto “…A che gioco giochiamo” in collaborazione con Associazione del Territorio.

Azioni da svolgere entro un'annualità scolastica

Organizzare dei momenti di presentazione del progetto Generazioni Connesse rivolto rispettivamente agli studenti, ai docenti, ai genitori.

Azioni da svolgere nei prossimi 3 anni

Organizzare un evento di presentazione, consultazione e conoscenza dell’ePolicy rivolto rispettivamente agli studenti, ai docenti e ai genitori.

Capitolo 2 - Formazione e curricolo

2.1. Curricolo sulle competenze digitali per gli studenti

I ragazzi usano la Rete quotidianamente, talvolta in modo più "intuitivo" ed "agile" rispetto agli adulti, ma non per questo sono dotati di maggiori "competenze digitali".

Infatti, "la competenza digitale presuppone l'interesse per le tecnologie digitali e il loro utilizzo con dimestichezza e spirito critico e responsabile per apprendere, lavorare e partecipare alla società. Essa comprende l'alfabetizzazione informatica e digitale, la comunicazione e la collaborazione, l'alfabetizzazione mediatica, la creazione di contenuti digitali (inclusa la programmazione), la sicurezza (compreso l'essere a proprio agio nel mondo digitale e possedere competenze relative alla cybersicurezza), le questioni legate alla proprietà intellettuale, la risoluzione di problemi e il pensiero critico" ("Raccomandazione del Consiglio europeo relativa alla competenze chiave per l'apprendimento permanente", C189/9, p.9).

Per questo la scuola si impegna a portare avanti percorsi volti a promuovere tali competenze, al fine di educare gli studenti e le studentesse verso un uso consapevole e responsabile delle tecnologie digitali. Ciò avverrà attraverso la progettazione e implementazione di un curricolo digitale.

Il Curricolo sulle competenze digitali della scuola del Primo Ciclo di Istruzione è trasversale alle discipline previste dalle Indicazioni Nazionali: la competenza digitale è ritenuta dall'Unione Europea competenza chiave, per la sua importanza e pervasività nel mondo d'oggi.

Avere competenza digitale significa padroneggiare le nuove tecnologie, ma soprattutto usarle con "autonomia e responsabilità" nel rispetto degli altri.

Le raccomandazioni Europee ci ricordano la dimensione integrata degli aspetti tecnologici, cognitivi ed etici che coesistono nelle competenze digitali: - dimensione tecnologica: le tecnologie digitali sono indubbiamente strumenti per la risoluzione di molteplici problemi della vita quotidiana, ma possiedono una "grammatica" che occorre gradualmente imparare a conoscere; - dimensione cognitiva: essa 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: fa riferimento sia alla capacità di gestire in modo sicuro i dati personali e altrui che alle abilità socio-comunicative e partecipative per maturare una maggiore consapevolezza sui nostri doveri nei riguardi di coloro con cui comunichiamo online.

Nell'ambito del PNSD (paragrafo 4.2. sulle "Competenze e contenuti") l'Istituto si propone un programma di progressiva educazione alla sicurezza online come parte del curriculum scolastico. Si impegna a sviluppare una serie di competenze e comportamenti, tra cui:

● progettare attività e laboratori di Coding;

● sviluppare strategie per insegnare a valutare e verificare le informazioni per accettarne l'esattezza;

● capire la necessità di mettere in atto un comportamento corretto anche quando si utilizza un ambiente online;

● sapere che le identità online possono essere false e ingannevoli;

● comprendere che le informazioni personali pubblicate online sono vulnerabili; conoscere le principali regole che tutelano la privacy delle persone; con particolare attenzione al web, conoscere le principali regole del copyright;

● comprendere l'impatto di bullismo online, sexting, grooming e sapere come cercare aiuto in caso di pericolo;

● sapere come segnalare eventuali abusi on-line e come chiedere aiuto agli adulti.

Il DigComp 2.1, nello specifico ne "Il quadro di riferimento per le competenze digitali dei cittadini" si elencano ben otto livelli di padronanza per ciascuna delle seguenti aree della cittadinanza digitale:

1. Alfabetizzazione e dati: ovvero la capacità di cercare, selezionare e valutare le informazioni in Rete;

2. Comunicazione e collaborazione: saper riconoscere le giuste e appropriate modalità per comunicare e relazionarsi online;

3. Creazione di contenuti digitali: valutare le modalità più appropriate per modificare, migliorare e integrare contenuti e informazioni, creandone di nuovi e originali;

4. Sicurezza: imparare a proteggere i dati personali e i contenuti digitali, comprendendo i rischi e le minacce presenti negli ambienti digitali.

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.

Tra i principali vantaggi legati all'utilizzo delle TIC nella didattica vi sono:

1. la motivazione e il coinvolgimento attivo da parte degli alunni;
2. la facilitazione dei lavori di gruppo e del confronto fra pari;
3. l'arricchimento della proposta didattica e supporto all'apprendimento per gli studenti con Bisogni Educativi Speciali.

Il nostro Istituto promuove la formazione personale dei docenti con corsi sull'uso delle TIC in ambito territoriale, ma anche interni alla scuola stessa, avvalendosi delle risorse di docenti esperti. Supporta anche l'auto aggiornamento dei singoli docenti.

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.

L'Istituto intende prevedere, nel corso del triennio, specifici momenti di formazione

personale e collettiva per i docenti, unitamente a momenti formativi di approfondimento (laboratori, eventi, giornate, ecc…) con le famiglie e gli studenti, per sensibilizzare l'intera comunità educante.

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 quindi si impegna: - alla diffusione delle informazioni e delle procedure contenute nel documento di ePolicy; - ad offrire incontri e conferenze con esperti interni ed esterni; - a fornire sul sito https://www.icmontaltotaverna.edu.it un link per essere costantemente informati su progetti, attività e iniziative di sensibilizzazione e prevenzione al bullismo/cyberbullismo.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2022/2023)

- 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 dei tre anni scolastici successivi)

- 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.

Sono "dati personali" le informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona e che possono fornire molteplici informazioni sul suo conto (dai dati anagrafici a quelli "sensibili", di natura religiosa, etnica… fino a quelli giudiziari). Il "trattamento" di questi dati sono l'insieme di operazioni, digitalizzate e non, applicate ad essi e l'istituzione scolastica può trattare solamente i dati personali necessari al perseguimento di specifiche finalità istituzionali o quelli previsti dalla norma di settore. Un esempio di violazione della protezione dei dati personali è il trattamento di questi senza aver fornito all'interessato un'adeguata informativa in merito, o senza aver ricevuti uno specifico consenso.

Il nostro Istituto prevede due modelli: per il trattamento dei dati personali di studenti/genitori ed uno specifico per il personale.

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.

La Rete internet della scuola è gestita dal Comune di Montalto Uffugo. L'Istituto dispone in tutte le sue sedi di una rete internet, cui accedono i computer e le Lim delle aule e dei laboratori (rete didattica) separatamente da quelli dell'amministrazione (rete segreteria). L'ottenimento delle credenziali per l'utilizzo della rete wifi è riservato ai docenti e al personale dell'Istituto. Le regole di comportamento sono analoghe a quelle per la connessione alle reti cablate di Istituto. Non è previsto l'accesso al wi-fi della scuola per gli studenti, che possono utilizzare la rete esclusivamente in presenza dei docenti, attraverso gli strumenti informatici in dotazione nella scuola.

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.

Al fine di favorire la comunicazione, nel nostro Istituto si utilizzano: sito web istituzionale https://www.icmontaltotaverna.edu.it, registro elettronico Argo, posta elettronica.

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.

La scuola non consente l'utilizzo del cellulare personale degli alunni all'interno dell'Istituto e in orario scolastico, se non su esplicita autorizzazione del docente e per determinate attività didattiche, previo accordo con studenti/esse e genitori; la scuola deve chiedere ai genitori dei minori di 13 anni di età il consenso all'uso di Internet a scuola per il loro figlio e per la pubblicazione dei suoi lavori e delle sue fotografie. Per i docenti e per il personale della scuola è consentito l'uso dello smartphone e di altri dispositivi elettronici personali durante le ore di lezione solo a scopo didattico ed integrativo di quelli scolastici disponibili.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2022/2023).

- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

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

- Organizzare incontri per la consultazione degli studenti/studentesse su 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 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.*

Il nostro Istituto, considerate le molteplici problematiche sociali che si manifestano in rete, con modalità differenti a seconda del target di riferimento, si impegna nella sensibilizzazione sui temi del cyberbullismo e dei principali rischi legati ad un utilizzo non consapevole e non responsabile della rete. Per quanto riguarda gli interventi di prevenzione, essi si distingueranno in azioni di prevenzione universale, selettiva e

indicata.

In particolare l'Istituto si impegna ad approfondire i seguenti temi, all'interno delle classi, con le modalità scelte dai singoli consigli di classe e di interclasse:

- gestione delle relazioni/affettività/sessualità;

- la diversità;

- le emozioni;

- l'uso sicuro, responsabile e consapevole delle tecnologie digitali;

- il senso del limite e la legalità.

Per la "prevenzione selettiva" (con interventi mirati, da attivare in presenza di rischio individuato), si lavorerà nelle singole classi con le modalità scelte dal consiglio di classe o di interclasse e/o in accordo con il Dirigente scolastico, il referente Bullismo e Cyberbullismo e la psicologa di Istituto.

La "prevenzione indicata" (rivolta a singoli studenti in presenza di specifici episodi connessi ad un utilizzo improprio della rete), si attuerà secondo i criteri scelti dal consiglio di classe o di interclasse e comunque sentito prima il parere del Dirigente scolastico.

Nei percorsi di prevenzione (sia essa universale, selettiva o indicata) la scuola valuta se stabilire specifici accordi con la rete dei servizi locali (ASP e Polizia Postale).

4.2 - Cyberbullismo: che cos'è e come prevenirlo

La legge 71/2017 "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo", nell'art. 1, comma 2, definisce il cyberbullismo:

"qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo".

La stessa legge e le relative **Linee di orientamento per la prevenzione e il contrasto del cyberbullismo** indicano al mondo scolastico ruoli, responsabilità e

azioni utili a prevenire e gestire i casi di cyberbullismo. Le linee prevedono:

- formazione del personale scolastico, prevedendo la partecipazione di un proprio referente per ogni autonomia scolastica;
- sviluppo delle competenze digitali, tra gli obiettivi formativi prioritari (L.107/2015);
- promozione di un ruolo attivo degli studenti (ed ex studenti) in attività di peer education;
- previsione di misure di sostegno e rieducazione dei minori coinvolti;
- Integrazione dei regolamenti e del patto di corresponsabilità con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti;
- Il sistema scolastico deve prevedere azioni preventive ed educative e non solo sanzionatorie.
- **Nomina del Referente per le iniziative di prevenzione e contrasto che:**
    - Ha il compito di coordinare le iniziative di prevenzione e contrasto del cyberbullismo. A tal fine, può avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio.
    - Potrà svolgere un importante compito di supporto al dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d'istituto), atti e documenti (PTOF, PdM, Rav).

Il nostro Istituto, anche attraverso la figura del referente bullismo e cyberbullismo e dell'animatore digitale, interviene:

- promuovendo lo sviluppo delle competenze digitali e di cittadinanza digitale;

- sostenendo azioni di educazione all'uso sicuro, consapevole e responsabile delle tecnologie digitali e dei social media;

- integrando con contenuti o riferimenti specifici il sito web ufficile dell'Istituto;

- integrando il Regolamento e il Patto di Corresponsabilità con specifici riferimenti a condotte di cyberbullismo e relative sanzioni;

- mantenendo un dialogo collaborativo con le famiglie;

- attivando interventi di prevenzione universale, selettiva e indicata;

- attivando misure di sostegno sulle persone coinvolte.

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.

Tale fenomeno, particolarmente diffuso e insidioso, non meno grave della sua espressione offline, è più difficile da individuare e combattere. La diffusione di messaggio di incitamento all'odio è maggiormente tollerata in Internet, che è meno sottoposto a controlli. ll discorso d'odio procura sofferenza in chi lo subisce e ha indubbiamente radici profonde, che devono essere individuate e "smantellate". Lo sviluppo delle competenze digitali e l'educazione ad un uso etico e consapevole delle tecnologie assumono un ruolo centrale per la promozione della consapevolezza di queste dinamiche in Rete.

Il nostro Istituto si impegna a fornire ai più giovani gli strumenti necessari per decostruire gli stereotipi su cui spesso si formano forme di hate speech e promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e il social network.

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?

Il nostro Istituto si impegna ad attivare una indagine su una eventuale dipendenza da internet e dal gioco online e a lavorare sul tema dell'adolescenza (anche con approccio curricolare), attivando percorsi di approfondimento mirati a raggiungere una condizione di benessere digitale.

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.

Il nostro Istituto promuove negli alunni lo sviluppo di quella consapevolezza necessaria alla prevenzione del fenomeno del Sexting.

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.

L' Istituto intende accompagnare gli studenti in un percorso di educazione (anche digitale) all'affettività, attraverso l'approfondimento, anche in chiave curriculare, con l'obiettivo di promuovere lo sviluppo di capacità nella gestione e protezione della propria privacy e della propria identità online e di favorire l'individuazione da parte degli stessi alunni di potenziali rischi di adescamento 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.

Il dialogo e la condivisione di regole (adeguate all'età) sull'uso delle tecnologie sono fondamentali per un'educazione positiva all'utilizzo delle tecnologie e la prevenzione deve cominciare presto,dato che viviamo circondati dalle tecnologie digitali. Essere consapevole dei rischi che si annidano online, è un primo importante passo per navigare e saper riconoscere un pericolo. Supportare bambini e adolescenti nella gestione della propria identità online è fondamentale per gli adulti di riferimento. Parlare, interessarsi e prevenire sono le parole chiave per evitare di trovarsi coinvolti in situazioni rischiose.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2022/2023).

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

☐ Organizzare uno o più incontri informativi per la prevenzione dei rischi

associati all'utilizzo delle tecnologie digitali, rivolti agli/lle studenti/studentesse, con il coinvolgimento di esperti.

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

□ 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.

□ Pianificare e realizzare progetti di peer-education - sui temi della sicurezza online - nella 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/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.

L' Istituto si impegna a porre attenzione alla rilevazione di rischi connessi alla navigazione sul web e all'uso improprio dei social network, con particolare riferimento ai fenomeni di cyberbullismo, all'adescamento 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.

E' importante che nell'Istituto siano facilmente reperibili la scheda di Osservazione per fenomeni afferenti a bullismo e cyberbullismo e la scheda per la Segnalazione del presunto caso di bullismo e cyberbullismo. E' altresì possibile comunicare direttamente con gli insegnanti della Commissione Bullismo, con la psicologa dello sportello di ascolto, la vicepreside o il Dirigente Scolastico, che si faranno da tramite. Quando si viene a conoscenza di un problema di bullismo e cyberbullismo non è opportuno che il singolo intraprenda iniziative personali, come ad esempio interrogare bulli e/o le vittime: occorre rivolgersi alla Commissione che prenderà in carico il problema. La segnalazione alle autorità competenti può avvenire su iniziativa della famiglia del minore coinvolto o può essere fatta dalla scuola.

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

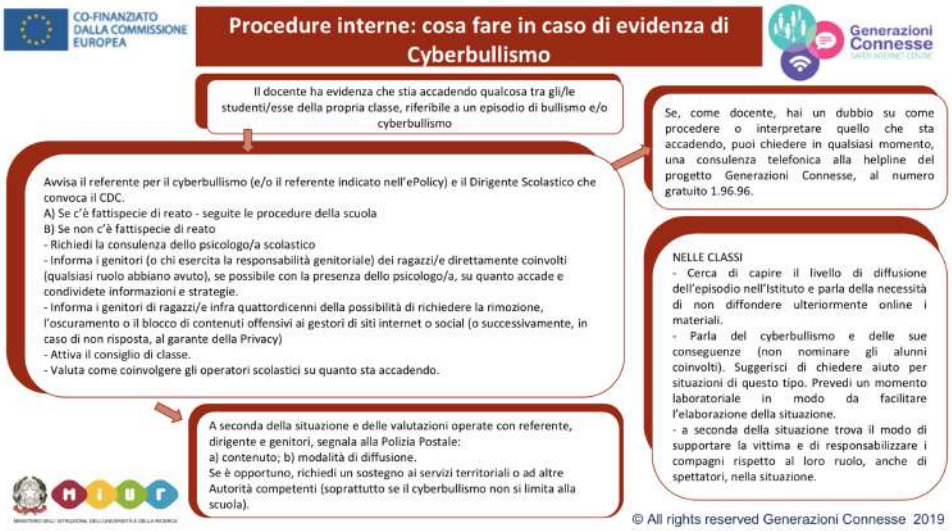
particolare attenzione alla tutela dei minori.

- **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.

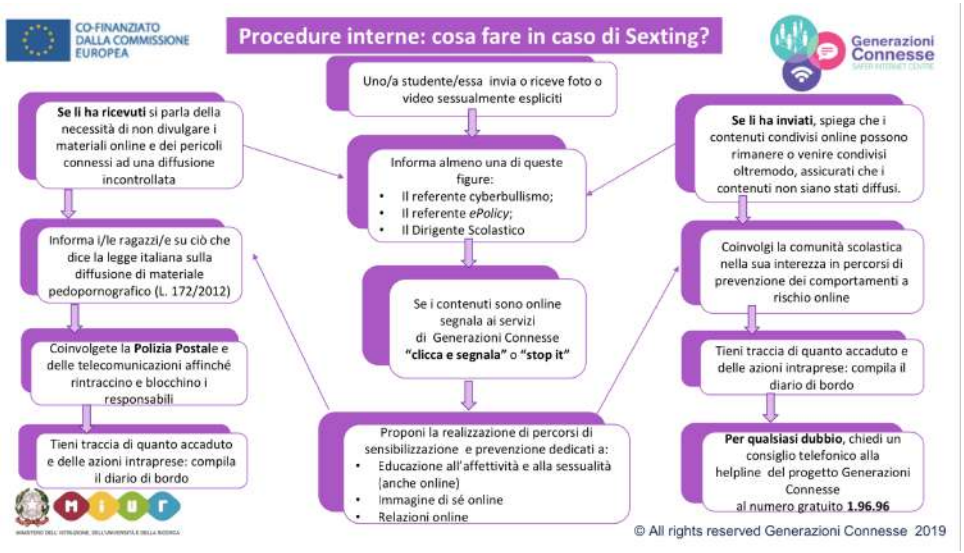
Attualmente nel nostro Istituto esistono prassi informali di comunicazione con le autorità competenti e con i servizi socio-sanitari del territorio per la gestione condivisa di episodi e/o comportamenti a rischio associati all'utilizzo delle tecnologie digitali.

5.4. - Allegati con le procedure

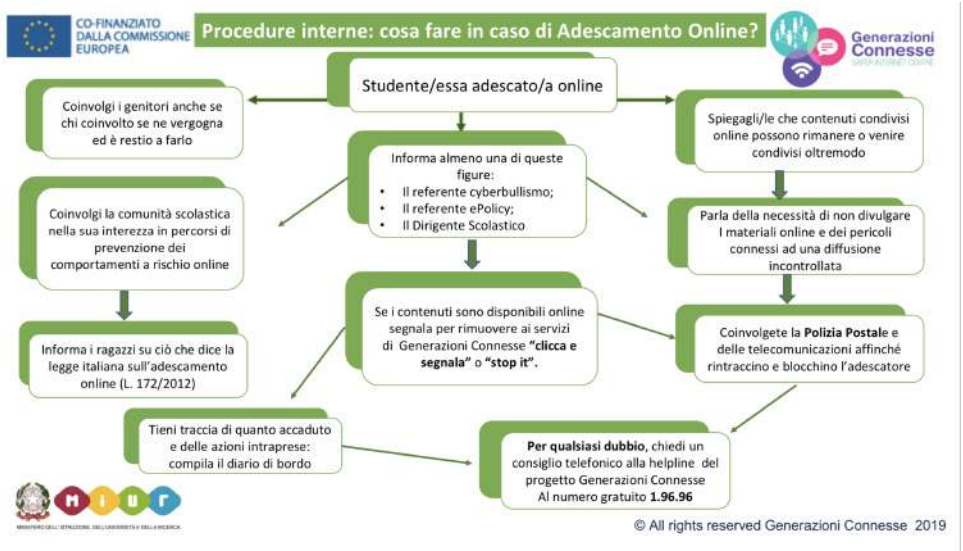
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



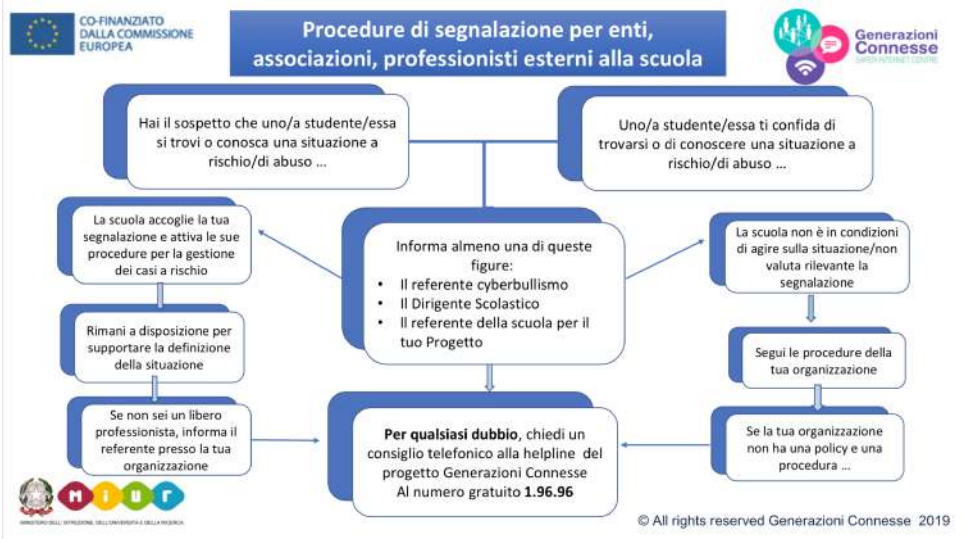
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



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



Altri allegati

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

1. SCHEDA DI OSSERVAZIONE PER LA RILEVAZIONE DI EVENTUALI SITUAZIONI PROBLEMATICHE IN CLASSE RICONDUCIBILI A BULLISMO /CYBERBULLISMO
2. SCHEDA DI SEGNALAZIONE SITUAZIONE DI BULLISMO/CYBERBULLISMO

Il nostro piano d'azioni

Sulla base delle "Linee guida per l'uso positivo delle tecnologie digitali e della prevenzione dei rischi nelle scuole", vengono assunti i seguenti punti per una collaborazione sinergica tra scuola-famiglia-servizi territoriali, al fine di creare un modello sinergico di azioni condivise:

- coinvolgimento di tutti gli attori della scuola: studenti, docenti, genitori e personale ATA, per l'affermazione di un modello di scuola come comunità;

- alleanza educativa tra scuola e famiglia;

- interventi educativi ed azioni di supporto, quale prevenzione per eventuali comportamenti a rischio.