Documento di ePolicy

CTIS01700V

IS G. B. VACCARINI

VIA ORCHIDEA 9 - 95123 - CATANIA - CATANIA (CT)

Salvina Gemmellaro

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.

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.

La scuola è una comunità educante il cui scopo principale è l'**educazione della persona** intesa come l'insieme delle azioni formative aventi come scopo la **valorizzazione della personalità individuale di ciascun studente e di ciascuna studentessa**. Ogni persona che, a vario titolo, ha un ruolo all'interno della comunità è portatrice di contributi che comportano responsabilità ben individuate. Anche enti esterni ed associazioni che occasionalmente collaborano con la scuola per progetti formativi e culturali, assumono delle responsabilità nei confronti degli studenti e delle studentesse definite in questo documento.

Propone la sottoscrizione espressa, in apposito modulo, della presa visicone dell' EPOLICY dell'Istituto.

Dirigente Scolastico

È il garante della sicurezza, anche online, di tutti i membri della comunità scolastica. Promuove la cultura della sicurezza online e fornisce il proprio contributo all'organizzazione, insieme al docente referente sulle tematiche del bullismo/cyberbullismo, di corsi di formazione specifici per tutte le figure scolastiche sull'utilizzo positivo e responsabile delle TIC. Gestisce ed interviene nei casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali.

Animatore digitale

Supporta il personale scolastico da un punto di vista tecnico-informatico dei rischi online e coadiuva il Dirigente Scolastico riguardo la protezione e gestione dei dati personali. Contribuisce alla promozione di percorsi di formazione interna all'Istituto negli ambiti di sviluppo della delle competenze digitali. Gestisce e amministra le piattaforme didattiche dell'Istituto (G Suite for Education e Office 365 for Education) monitorandone gli accessi ai fini della sicurezza degli studenti e delle studentesse e degli operatori scolastici.

Referente bullismo e cyberbullismo

In osservanza all'art. 4 Legge n.71/2017, "Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo" coordina e promuove iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo. Può, pertanto, avvalersi della collaborazione delle Forze di polizia, delle associazioni e dei centri di aggregazione giovanile del territorio. Può coinvolgere, con progetti e percorsi formativi ad hoc, studenti, colleghi e genitori. Supporta il dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d'istituto), atti e documenti (PTOF, PdM, Rav).

Propone di inserire, in seno al Patto di Corresponsabilità, con dicitura nel Documento "VIVAMENTE RACCOMANDATO", l'organizzazione di corsi informativi con Forze dell'ordine ed associazioni di professionisti del settore,dedicati alle famiglie, quale guida operativa nell'opera educativa dei propri figli.

Docenti

Hanno la responsabilità di diffondere la cultura dell'uso responsabile delle TIC e della Rete integrando parti del curriculum della propria disciplina con approfondimenti ad hoc. Accompagnano e supportano gli studenti e le studentesse nelle attività di apprendimento e nei laboratori che prevedono l'uso di dispositivi tecnologici che si connettono alla Rete. Segnalano al Dirigente Scolastico qualunque problematica, violazione o abuso, anche online, che vede coinvolti studenti e studentesse.

Personale amministrativo, tecnico e ausiliario (ATA)

Secondo il proprio ruolo (amministrativo, contabile, gestionale e di sorveglianza), in collaborazione con il dirigente scolastico e con il personale docente, si occupa, ciascuno per la propria funzione, del funzionamento dell'Istituto scolastico anche attraverso lo sviluppo della cultura digitale e dell'organizzazione del tempo scuola. Adeguatamente formato (e/o auto-formato) in materia di bullismo e cyberbullismo è coinvolto nella segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo, secondo i regolamenti interni d'Istituto. Insieme ad altre figure può contribuire a raccogliere, verificare e valutare le informazioni inerenti possibili casi di bullismo/cyberbullismo.

Studenti e studentesse

In base al grado di maturità e consapevolezza raggiunta, hanno il dovere di utilizzare al meglio le tecnologie digitali in coerenza con quanto richiesto dai docenti. Si impegnano a imparare a tutelarsi online, a tutelare i/le propri/e compagni/e e rispettarli/le; per quanto possibile, partecipano attivamente a progetti ed attività che riguardano l'uso positivo delle TIC e della Rete e farsi promotori di quanto appreso anche attraverso possibili percorsi di peer education.

Genitori

Possono partecipare alle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete e sull'uso responsabile dei device personali. Si relazionano in modo costruttivo con i docenti sulle linee educative che riguardano le TIC e la Rete, comunicando anche gli eventuali problemi rilevati quando i/le propri/e figli/e non usano responsabilmente le tecnologie digitali o Internet.

Enti esterni e associazioni

Si conformano alla politica della scuola riguardo all'uso consapevole della Rete e delle TIC. Promuovono comportamenti sicuri, la sicurezza online e assicurare la protezione degli studenti e delle studentesse durante le attività extracurricolari. Pertanto, nei protocolli d'intesa e nei contratti di collaborazione, gli enti esterni si impegnano ad accogliere e rispettare le norme stabilite da questo documento a salvaguardia dei dati personali e sensibili degli studenti e delle studentesse e al fine di prevenire o intervenire in casi di uso non idoneo delle tecnologie digitali.

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).

Per garantire la sicurezza informatica degli studenti e delle studentesse dell'Istituto Scolastico "Giovan Battista Vaccarini", i soggetti che collaborano con la scuola per

attività formative, culturali, sportive e di percorsi per le competenze trasversali e per l'orientamento sono tenuti a sottoscrivere l'Informativa predisposta dall'Istituto che, seppur adattata alle specifiche attività previste in convenzione, non possono prescindere dai seguenti punti:

1. Premessa e obiettivi dell'Informativa.
   L'Informativa è formulata a tutela della sicurezza informatica degli studenti e delle studentesse riguardo i propri dati personali e prevenire qualsiasi forma di utilizzo scorretto delle risorse digitali in Rete che possano provocare danni morali e materiali agli utilizzatori stessi. Essa mira ad individuare regole condivise in materia di prevenzione, intervento e segnalazione di casi che possano verificarsi durante le attività formative.
2. Destinatari (organizzazioni e soggetti esterni).
3. Ambiti di applicazione e Ruoli
   Specificare sinteticamente il progetto specifiche e/o le attività previste
   Individuare i docenti di riferimento del progetto specifico o delle attività
4. Regolamento / Codice di comportamento.
    1. Il soggetto esterno che collabora con l'Istituto condivide le medesime finalità della scuola in materia di sicurezza delle informazioni e dei dati riguardanti gli studenti e le studentesse della scuol
    2. Il soggetto esterno si impegna ad utilizzare le risorse didattiche digitali secondo le norme stabilite dalla ePolicy della scuola. In particolare:
        - Le piattaforme di didattica digitale utilizzate dal soggetto esterno, qualora non venga effettuato con quelle dell'Istituto, deve rispondere alle norme di sicurezza stabilite dalla normativa vigente e, pertanto, devono essere iscritte nel Cloud Marketplace AgID.
        - L'utilizzo dei dispositivi personali (smartphone, tablet, pc, etc.) degli studenti e delle studentesse e quelli in dotazione della scuola devono essere utilizzati secondo le finalità precipue dell'attività formativa/culturale, evitando un uso improprio o comunque deontologicamente scorretto durante le attività.
    3. Il personale esterno che svolge il ruolo di tutor o di esperto deve mantenere un alto profilo professionale e, pertanto, in ogni sessione prevista dal calendario delle attività pattuito con la scuola, si impegna a erogare il proprio servizio professionale esclusivamente agli studenti e alle studentesse dell'Istituto. Resta salva la facoltà di derogare tale norma in caso di diversa prestazione prevista nell'accordo fra la scuola e l'ente erogatore (ad esempio, formazione che coinvolga reti di scuole, collaborazione fra enti e scuole, etc.)
    4. Il comportamento di ogni studente e di ogni studentessa deve essere sempre adeguato alla circostanza: non sono tollerati atteggiamenti irrispettosi fra pari e verso le persone che erogano formazione, violazioni di privacy, attacchi alla persona, insulti, ingiurie, bestemmie. In caso di manifestazioni non consone al presente Regolamento, l'ente è

tenuto a segnalare alla scuola quanto accaduto secondo le modalità descritte al punto 5.

5. Il soggetto esterno si impegna a non divulgare a terzi i dati personali e quelli sensibili eventualmente emersi durante le attività extracurricolari e di non utilizzarli se non per gli esclusivi scopi dell'attività pattuita in sede di accordo/convenzione. Il soggetto esterno si obbliga, pertanto, a 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).
6. Procedure di segnalazione
   In caso di sospetto e acclarato fenomeno di bullismo, cyberbullismo o qualsiasi altra forma di prevaricazione ripetuta nel tempo, il soggetto erogatore deve immediatamente segnalare il fatto ad almeno una delle seguenti figure: il referente per il cyberbullismo della scuola, il dirigente scolastico, il referente del progetto della scuola.
   Allegare i moduli di segnalazione per le situazioni di rischio
7. Provvedimenti nel caso di omessa segnalazione
   Qualora il soggetto esterno non provvedesse a segnalare l'eventuale caso di bullismo o cyberbullismo, per negligenza o colpa o dolo, la scuola riterrà risolto l'accordo e si riserva di rivalersi sull'ente esterno in sede penale e civile in caso di conseguenze legali del caso non segnalato.
8. Provvedimenti nel caso di violazione del codice di comportamento

- Qualora la scuola riscontrasse provate violazioni al presente Regolamento da parte del personale afferente al soggetto esterno, essa si riserva di procedere a formale segnalazione alle Autorità competente (Polizia postale, Tribunale per i minorenni, Garante della Privacy) a tutela dei propri studenti e delle proprie studentesse.
- Qualora la violazione del codice di comportamento fosse compiuta da uno studente o da una studentessa, accertata dalla scuola o segnalata dal soggetto esterno, la scuola esperirà le procedure correttive e disciplinari stabilite dall'ePolicy e dal Regolamento di Istituto.

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.

I docenti, il Personale ATA, gli studenti e le studentesse sono invitati a promuovere il documento nell'Istituto e all'esterno, affinché la cultura del *buon uso delle risorse digitali* possa essere proficuamente disseminata.

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.

Il documento di riferimento è il Regolamento di Istituto condiviso con le famiglie e sottoscritto attraverso il Patto di corresponsabilità.

1.6 - Integrazione dell'ePolicy con Regolamenti esistenti

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

I documenti indicati possono essere consultati ai seguenti link:

- Regolamento di Istituto
- Patto di Corresponsabilità

1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

L'E-policy viene aggiornata periodicamente e quando si verificano cambiamenti significativi in riferimento all'uso delle tecnologie digitali all'interno della scuola. Le modifiche del documento saranno discusse con tutti i membri del personale docente. Il monitoraggio del documento sarà realizzato a partire da una valutazione della sua efficacia in riferimento agli obiettivi specifici che lo stesso si pone.

La Dirigente Scolastica può nominare un docente in qualità di referente per la revisione e/o l'aggiornamento della presente ePolicy.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i docenti dell'Istituto per la stesura finale dell'ePolicy.

Azioni da svolgere nei prossimi 3 anni:

- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i docenti dell'Istituto per la stesura finale dell'ePolicy.
- Organizzare incontri per la consultazione degli studenti/studentesse sui temi dell'ePolicy per cui si evidenzia la necessità di regolamentare azioni e comportamenti di presentazione del progetto Generazioni Connesse.
- Organizzare uno o più eventi o attività volti a presentare l'ePolicy ai genitori dell'Istituto e di presentazione del progetto Generazioni

Connesse.

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.

Per quanto concerne la progettazione del curricolo digitale, il Collegio dei docenti definirà le linee guida che i singoli dipartimenti disciplinari declineranno in termini di obiettivi specifici di apprendimento. Sarà poi facoltà di ogni Consiglio di classe perseguire, anche in modo trasversale le singole discipline, le competenze digitali secondo il ***DigComp 2.1***.

In particolare, effettuata un'accurata analisi dei fabbisogni cognitivi, il Collegio dei docenti individuerà un ordine di priorità delle competenze digitali secondo la **dimensione tecnologica** (le tecnologie digitali come strumenti per la risoluzione di problemi della vita quotidiana e l'adeguata comprensione della "grammatica" dello strumento onde evitare automatismi che abbiano conseguenze incerte), quella **cognitiva** (la capacità di cercare, usare e creare in modo critico le informazioni condivise in Rete, valutandone credibilità e affidabilità) e quella **etica** e **sociale** (la prima si riferisce alla capacità di gestire in modo sicuro i propri dati personali e quelli

altrui, e di usare le tecnologie digitali per scopi eticamente accettabili e nel rispetto degli altri; la seconda riguarda lo sviluppo di particolari abilità socio-comunicative e partecipative per maturare una maggiore consapevolezza sui doveri nei riguardi di coloro con cui si comunica online) da inserire nel curricolo digitale di Istituto. I singoli dipartimenti svilupperanno percorsi comuni che possono essere interdisciplinari e potranno indicare anche i modi e i tempi di attuazione. Sarà compito, quindi del Consiglio di classe attuare i percorsi sviluppandoli con attività strutturate e ben definite.

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 collegio dei docenti riconosce e favorisce la partecipazione del personale ad iniziative promosse sia direttamente dalla scuola (ad es. con l'aiuto dell'animatore digitale) dalle reti di scuole e dall'amministrazione, sia quelle liberamente scelte dai docenti (anche online), purché restino coerenti con il piano di formazione. Le TIC, infatti, potranno essere usate in modo strutturato dagli insegnanti ad integrazione della didattica al fine di progettare, sviluppare, utilizzare, gestire e valutare i processi di insegnamento e apprendimento di tutti gli studenti e le studentesse della classe, anche delle persone con disabilità (in chiave inclusiva) e promuovere lo sviluppo di importanti capacità richieste in ambito lavorativo, come il lavoro di gruppo anche a distanza e il confronto fra pari in modalità asincrona.

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.

Particolare attenzione verrà posta alla condivisione di buone pratiche nell'utilizzo consapevole delle TIC al fine di prevenire e contrastare ogni forma di discriminazione, offesa, denigrazione e lesione della dignità dell'altro, nonché fenomeni di bullismo e cyberbullismo.

A seguito di un'attenta analisi dei fabbisogni formativi del personale docente, verranno programmati momenti di formazione che, oltre eventuali alfabetizzazioni e approfondimenti sull'uso degli strumenti digitali online, riguarderanno anche la sfera emotiva e affettiva degli studenti e delle studentesse che usano le nuove tecnologie in modo da educare alle emozioni nel contesto online e modulare e gestire i propri ed altrui comportamenti.

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.

In particolare,

- verranno puntualizzate le **regole sull'uso delle tecnologie digitali** da parte dei genitori nelle comunicazioni con la scuola e con i docenti e definite chiaramente le medesime regole che riguardano gli studenti e studentesse;
- saranno informati i genitori sui **consigli o linee guida sull'uso delle tecnologie digitali nella comunicazione** con i figli e in generale in famiglia;
- potranno essere organizzati **percorsi di sensibilizzazione e formazione** dei genitori sull'uso responsabile e costruttivo della Rete in famiglia e a scuola anche con il coinvolgimento degli studenti e delle studentesse.

Il nostro piano d'azioni

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

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

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

- 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.

Le informative rivolte, tra gli altri, alle famiglie e agli enti esterni sono reperibili sul sito web della scuola all'indirizzo https://netcrm.netsenseweb.com/scuola/privacy/netsense/CTIS01700V.

In riferimento all'uso delle tecnologie digitali, la scuola non richiede e non permette agli alunni l'attivazione di qualsivoglia account che non sia esclusivamente quello relativo alla piattaforma istituzionale o per la partecipazione a eventi o progetti rientranti nell'offerta formativa della scuola. L'utilizzo della rete dati avviene in totale sicurezza, grazie al mantenimento degli standard previsti da AGID "Misure minime di sicurezza ICT per le PA" e all'utilizzo di opportuni firewall che tracciano il traffico e filtrano i siti non opportuni e non idonei per le attività didattiche. I dati trattati durante tali attività sono quelli derivanti da tracciamenti (log) delle attività di navigazione e a disposizione esclusivamente delle autorità giudiziarie nel caso di loro esplicita richiesta.

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.

Tale diritto è garantito dalla scuola a tutti gli studenti e a tutte le studentesse attraverso un'infrastruttura di rete a banda ultra larga e Wi-Fi filtrato mediante firewall. Gli studenti e le studentesse possono accedere alla rete Internet esclusivamente per scopi didattici e all'interno di unità di apprendimento che prevedano ricerche e strumenti di collaborazione online, sia attraverso dispositivi digitali forniti dalla scuola, sia mediante dispositivi digitali personali (BYOD). Ciò è normato dal Regolamento di Istituto (*cfr*. art. 21 comma 8) che recita:
"Riguardo i dispositivi digitali:
a. l'uso in classe di strumenti tecnologici quali computer portatili, tablet e smartphone è consentito qualora l'insegnante prevede di attuare metodologie didattiche in cui l'utilizzo di dispositivi elettronici personali sia ritenuto proficuo ed efficace (ad esempio, BYOD: Bring Your Own Device). È inoltre permesso l'uso del computer portatile o tablet per gli studenti per i quali sono stati prescritti (o deliberati dal Consiglio di Classe) strumenti compensativi e/o dispensativi che prevedano l'uso di tali strumenti digitali per migliorare la qualità dell'apprendimento.
b. nell'ambito delle condizioni stabilite dal precedente comma, l'uso in classe di Internet è consentito solo per le finalità didattiche stabilite dall'insegnante.
c. l'utilizzo dei dispositivi elettronici, sia personali che dell'Istituto, per finalità che prescindono dalle attività didattiche o per attuare forme persecutorie o offensive della dignità delle persone (cyberbullismo), è tassativamente vietato e verrà punito con l'irrogazione di sanzioni classificate da S5 a S9 come previsto dall'art. 3 del Regolamento Attuativo dello Statuto delle Studentesse e degli Studenti in Appendice A oltre che denunciato all'Autorità di Polizia competente".

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.

Il principale strumento di comunicazione interna è costituito dal **registro elettronico** che, oltre alle comunicazioni inerenti agli argomenti delle lezioni, le consegne per casa, i promemoria, le note disciplinari e le valutazioni degli alunni/e, è utilizzato per inviare tutte le comunicazioni riservate alla singola classe o al singolo studente o alla singola studentessa. Anche le comunicazioni alle famiglie sono mediate dagli strumenti di comunicazioni forniti dal registro elettronico (e-mail, bacheche).

Altro strumento fondamentale con cui la scuola veicola le informazioni e le disposizioni al grande pubblico è il proprio **sito web** www.vaccarinict.edu.it. Esso, oltre a rendere disponibili al pubblico gli atti amministrativi necessari (A*lbo Pretorio* e *Amministrazione Trasparente)*, informa sulle iniziative didattiche e culturali della scuola, sugli eventi promozionali o di collaborazione con enti esterni e sulle attività formative extrascolastiche degli studenti. Le immagini e i dati personali riguardanti studenti e studentesse sono pubblicati sul sito web esclusivamente a scopo istituzionale e didattico.

La scuola utilizza anche *Twitter* per comunicare notizie del mondo della scuola di interesse pubblico, disposizioni di carattere generale e informazioni promozionali sulle iniziative dell'Istituto.

Inoltre, la scuola utilizza piattaforme online dotate di applicazioni che consentono di condurre le attività didattiche in modalità remota e di produrre propri materiali digitali. Le piattaforme adottate (***G Suite for Education*** e ***Microsoft Office 365 A1***), iscritte ad AgID Cloud Marketplace, garantiscono un certo grado di sicurezza interna grazie al monitoraggio da parte dell'amministrazione del traffico interno e quello con l'esterno. Ogni persona della scuola (studente, studentessa, docente, Personale ATA) possiede, in entrame le piattaforme, un proprio account nel dominio *vaccarinict.edu.it* per cui ciascuno ha una propria casella di posta elettronica e un proprio spazio di cloud computing. In particolare e solo nella piattaforma *G Suite for Education*, ogni alunno/a può comunicare con la propria e-mail esclusivamente all'interno del dominio, mentre il Personale può comunicare anche ad e-mail esterne all'organizzazione: ciò per facilitare le comunicazioni con le famiglie o "istituzionalizzare" le comunicazioni con enti esterni (associazioni culturali, enti partner per i PCTO). Nella piattaforma *Microsoft Office 365 A1* tutte le email possono

comunicare esclusivamente all'interno del dominio.

Altri strumenti informali di comunicazione online (messaggistica istantanea) possono essere utilizzati per veicolare informazioni e notizie all'interno di gruppi omogenei (chat di docenti, di consigli di classe, di staff della Dirigente) oppure gruppi docente-alunni/e. A tutti, in ogni caso, è richiesto di attenersi alle regole dettate dalla netiquette:

- comprendere e rispettare sempre le finalità del gruppo, scrivendo e pubblicando solo contenuti pertinenti a tali finalità;
- non pubblicare informazioni personali e dati sensibili di altri utenti;
- usare sempre un linguaggio adeguato e il più possibile chiaro e preciso per evitare fraintendimenti;
- evitare di affrontare in chat argomenti troppo complessi e controversi;
- evitare discussioni di questioni che coinvolgono due o pochi interlocutori, onde evitare di annoiare e disturbare gli altri componenti del gruppo;
- non condividere file multimediali troppo pesanti;
- evitare di condividere foto di studenti in chat;
- indirizzare solo domande precise e chiare, a cui si possano dare risposte altrettanto brevi e precise;
- evitare messaggi troppo spezzettati, cercando il più possibile di essere brevi ed esaustivi allo stesso tempo.

Infine, si rammenta l'art. 22 (Livelli, soggetti, materie di relazioni sindacali per la Sezione Scuola) del CCNL 2016/2018, che fa riferimento ai criteri generali per l'utilizzo di strumentazioni tecnologiche di lavoro in orario diverso da quello di servizio, al fine di una maggiore conciliazione fra vita lavorativa e vita familiare ("diritto alla disconnessione"). Le deroghe a questa norma possono sussistere in presenza di eventi emergenziali e non differibili.

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.

A tal proposito, il Regolamento di Istituto prevede la possibilità che gli studenti e le studentesse possano portare a scuola il proprio dispositivo digitale (cfr. art. 21 comma 8 lett. a) per attuare metodologie didattiche in cui l'utilizzo di dispositivi elettronici personali sia ritenuto proficuo ed efficace. È inoltre permesso l'uso del computer portatile o tablet per gli studenti per i quali sono stati prescritti (o deliberati dal Consiglio di Classe) strumenti compensativi e/o dispensativi che prevedano l'uso di tali strumenti digitali per migliorare la qualità dell'apprendimento. Da ogni locale dell'Istituto è possibile accedere a Internet tramite Wi-Fi connesso a banda ultra-larga e filtrato da firewall opportunamente tarato per impedire navigazioni non sicure e potenzialmente pericolose. Ogni accesso alla Rete è tracciato e i file di log sono custoditi dal responsabile della protezione dei dati (DPO).

Il nostro piano d'azioni

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

- 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

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

- 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 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 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.*

La scuola si adopera affinché l'intera comunità scolastica conosca l'ePolicy con interventi mirati che consentano di prendere consapevolezza della situazione di fatto e della necessità di educare al buon uso delle risorse digitali, alla comunicazione online e alla cittadinanza digitale. Pertanto, la scuola considera prioritarie le azioni di promozione delle competenze digitali al fine di evitare l'insorgenza di rischi legati

all'utilizzo del digitale.

Nell'ottica di una prevenzione universale, gli organi collegiali (sia in sede di programmazione dipartimentale, sia nelle programmazioni didattiche dei consigli di classe) progetteranno azioni didattico-educative, anche a carattere interdisciplinare, che sviluppino le competenze digitali necessarie per l'educazione alla cittadinanza digitale. L'obiettivo è formare e consolidare le competenze educative di base necessarie a poter gestire le situazioni di vita che i/le ragazzi/e sperimentano online. La scuola può anche avvalersi del supporto delle diverse agenzie educative, come la famiglia, le istituzioni, le associazioni, la società civile, ciascuna con un proprio compito, secondo un progetto educativo condiviso.

Non vengono esclusi interventi di prevenzione selettiva rivolti a gruppi di studenti in cui il rischio online è presente e provato da circostanze reali documentate. Questi interventi prevedono programmi formativi strutturati che hanno l'obiettivo di migliorare le competenze digitali e le strategie di problem solving.

4.2 - Cyberbullismo: che cos'è e come prevenirlo

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

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

La stessa legge e le relative **Linee di orientamento per la prevenzione e il contrasto del cyberbullismo** indicano al mondo scolastico ruoli, responsabilità e azioni utili a prevenire e gestire i casi di cyberbullismo. Le linee prevedono:

- formazione del personale scolastico, prevedendo la partecipazione di un proprio referente per ogni autonomia scolastica;
- sviluppo delle competenze digitali, tra gli obiettivi formativi prioritari (L.107/2015);
- promozione di un ruolo attivo degli studenti (ed ex studenti) in attività di peer education;
- previsione di misure di sostegno e rieducazione dei minori coinvolti;

- Integrazione dei regolamenti e del patto di corresponsabilità con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti;
- Il sistema scolastico deve prevedere azioni preventive ed educative e non solo sanzionatorie.
- **Nomina del Referente per le iniziative di prevenzione e contrasto che:**
    - Ha il compito di coordinare le iniziative di prevenzione e contrasto del cyberbullismo. A tal fine, può avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio.
    - Potrà svolgere un importante compito di supporto al dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d'istituto), atti e documenti (PTOF, PdM, Rav).

Qualora la Dirigente Scolastica venga a conoscenza di atti di cyberbullismo, essa informa tempestivamente i genitori dei minori coinvolti (*cfr.* art.5 Legge 71/2017), a meno che il fatto costituisca reato. Non si esclude il supporto psicologico e/o di mediazione offerti dai servizi sociosanitari (ad esempio: Consultorio Familiare, servizi di Neuropsichiatria Infantile, centri specializzati sulla valutazione o l'intervento sul bullismo o in generale sul disagio giovanile, i comportamenti a rischio in adolescenza, etc.).

Per quanto riguarda la necessità di segnalazione e rimozione, 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 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. Il Garante ha pubblicato nel proprio sito il modello per la segnalazione/reclamo in materia di cyberbullismo da inviare a: cyberbullismo@gpdp.it.

Parallelamente, nel caso in cui si ipotizzi che ci si possa trovare di fronte ad una fattispecie di reato (come, ad esempio, il furto di identità o la persistenza di una condotta persecutoria che mette seriamente a rischio il benessere psicofisico del bambino/a o adolescente coinvolto/a in qualità di vittima) si potrà far riferimento agli uffici preposti delle Forze di Polizia per inoltrare la segnalazione o denuncia/querela e permettere alle autorità competenti l'approfondimento della situazione da un punto di vista investigativo. È in tal senso possibile far riferimento a queste tipologie di uffici: Polizia di Stato – Compartimento di Polizia postale e delle Comunicazioni; Questura o Commissariato di P.S. del territorio di competenza; Arma dei Carabinieri – Comando Provinciale o Stazione del territorio di competenza; Polizia di Stato – Commissariato online (attraverso il portale http:// www.commissariatodips.it oppure l'app YouPol).

Per un consiglio e un supporto è possibile rivolgersi alla Helpline di Telefono Azzurro

per *Generazioni Connesse*: operatori esperti e preparati sono a disposizione degli insegnanti, del Dirigente e degli operatori scolastici, oltre che degli adolescenti, dei genitori e di altri adulti che a vario titolo necessitano di un confronto e di un aiuto per gestire nel modo più opportuno eventuali esperienze negative e/o problematiche inerenti all'utilizzo dei media digitali.

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.

La consapevolezza di questo genere di dinamiche in rete può incrementarsi attraverso lo sviluppo delle competenze digitali e l'educazione ad un uso etico e consapevole delle tecnologie.

Le attività che la scuola si impegna a promuovere e realizzare, mirano, tra l'altro, a riconoscere e prevenire secondo i criteri su indicati questo tipo di fenomeni ed educare gli studenti e le studentesse alla partecipazione proattiva ai dibattiti sia in presenza che in quelli svolti in Rete.

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?

La scuola non sottovaluta questo aspetto che può compromettere seriamente la stabilità emotiva e psicologica della persona, soprattutto se insorge nell'età dello sviluppo e della maturazione cognitiva e comportamentale. E questo in un territorio dove gli stimoli esterni, dettati dalla carenza di prospettive lavorative gratificanti e dal prosperare di occasioni di guadagni che non comportano grandi sforzi fisici o culturali, sono pressanti e subdolamente seducenti.

Per questo, la scuola si adopera affinché siano attuate delle strategie idonee per un uso più consapevole delle tecnologie per favorire il "benessere digitale", cioè la capacità di creare e mantenere una relazione sana con la tecnologia, come

- la ricerca di equilibrio nelle relazioni anche online
- l'uso degli strumenti digitali per il raggiungimento di obiettivi personali
- la capacità di interagire negli ambienti digitali in modo sicuro e responsabile
- la capacità di gestire il sovraccarico informativo e le distrazioni (ad esempio, le notifiche)

Le attività che mirano allo sviluppo della cittadinanza digitale, alla prevenzione del cyberbullismo, all'uso integrativo e non sostitutivo dei dispositivi e della Rete, possono senz'altro includere le tematiche relative alla conoscenza e alla prevenzione della dipendenza da Internet e dal gioco online.

La scuola si impegna a integrare la tecnologia nella didattica, mostrandone l'utilizzo funzionale che può rendere più consapevoli i ragazzi e le ragazze delle proprie abitudini online e che può far raggiungere efficacemente i propri obiettivi. Questa integrazione può trovare attuazione mediante regole chiare e condivise stipulate fra docenti e alunni/e.

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.

La scuola si propone di sensibilizzare gli studenti e le studentesse su questa tematica che può essere sottovalutata e che può condurre a pericolosi risvolti futuri. Pertanto, nelle azioni informative e di prevenzione che la scuola proporrà, questo tema sarà particolarmente curato per sviluppare la consapevolezza dei gravi danni che questo fenomeno comporta, sia in termini psicologici che sociali, sia per il ragazzo/la ragazza soggetto della foto/del video che colui/coloro che contribuiscono a diffonderla/o. È importante che i giovani comprendano che azioni del genere rappresentano veri e propri comportamenti criminali perseguibili penalmente e con ripercussioni negative sulla vittima in termini di autostima, di credibilità, di reputazione sociale offline e online. A queste possono associarsi altri comportamenti a rischio, di tipo sessuale ma anche riferibili ad abuso di sostanze o di alcool. Inoltre, è importante conoscere che i rischi del sexting, legati al *revenge porn*, possono contemplare violenza psicosessuale, umiliazione, bullismo, cyberbullismo, molestie, stress emotivo che si riversa anche sul corpo insieme ad ansia diffusa, sfiducia nell’altro/i e depressione.

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.

Nelle azioni educative e formative inerenti questo documento che la scuola si propone di attuare, uno spazio è occupato da percorsi che sviluppino capacità per la protezione della propria privacy e per la gestione dell'immagine e dell'identità online, e di gestire adeguatamente le proprie relazioni online, di educazione (anche digitale) all'affettività e alla sessualità per accompagnare ragazze e ragazzi alla scoperta della propria sfera emotiva e personale, spesso costruita in modo distorto dai media o dalla carenza di un'adeguata educazione pregressa. L'obiettivo è aiutare a renderli più sicuri emotivamente e pronti ad affrontare eventuali situazioni a rischio, imparando innanzitutto a gestire le proprie emozioni, il rapporto con il proprio corpo e con gli altri. Inoltre, è fondamentale che imparino che c'è sempre un sicuro aiuto da parte di adulti (genitori e docenti) a cui potersi affidare che non li giudicano, ma li comprendono e li ascoltano. Perché ciò possa avvenire è necessario tenere sempre aperto un canale di comunicazione con loro sui temi dell'affettività, del digitale e della sessualità.

Nei casi sospetti o documentati è fondamentale che il computer o altri dispositivi elettronici del minore-vittima non vengano usati per non compromettere eventuali prove. Questi casi richiedono l'intervento della Polizia Postale e delle Comunicazioni a cui bisogna rivolgersi il prima possibile, tenendo traccia degli scambi fra il minore e l'adescatore (ad esempio, salvando le conversazioni attraverso screenshot, memorizzando eventuali immagini o video...). Data la delicatezza problematica non sono da escludere ripercussioni psicologiche significative sul minore. Per questo potrebbe essere necessario rivolgersi ad un Servizio territoriale (es. Consultorio Familiare, Servizio di Neuropsichiatria Infantile, ecc.) in grado di fornire alla vittima anche un adeguato supporto di tipo psicologico o psichiatrico.

Per consigli e per un supporto è possibile rivolgersi alla Helpline di *Generazioni Connesse* (**19696**): operatori esperti e preparati sono sempre a disposizione degli insegnanti, del Dirigente e degli operatori scolastici, oltre che dei bambini, degli adolescenti, dei genitori e di altri adulti che a vario titolo necessitano di un confronto e di un aiuto per gestire nel modo più opportuno eventuali esperienze negative e/o problematiche inerenti all'utilizzo dei nuovi media.

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.

Per maggiori approfondimenti, si invita a fare riferimento al Vademecum di *Generazioni Connesse*.

Il nostro piano d'azioni

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

Scegliere almeno 1 di queste azioni:

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

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

Scegliere almeno 1 di queste azioni:

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

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

□ 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.

□ 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.

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.

Le segnalazioni di casi personali o di casi sospetti di fenomeni in cui un compagno o una compagna siano vittime di prevaricazioni, possono essere inviate dagli studenti e dalle studentesse all'indirizzo di posta elettronica aiuto@vaccarinict.edu.it.

Alla medesima email possono fare riferimento anche i genitori, il Personale docente e il Personale ATA dell'Istituto.

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.

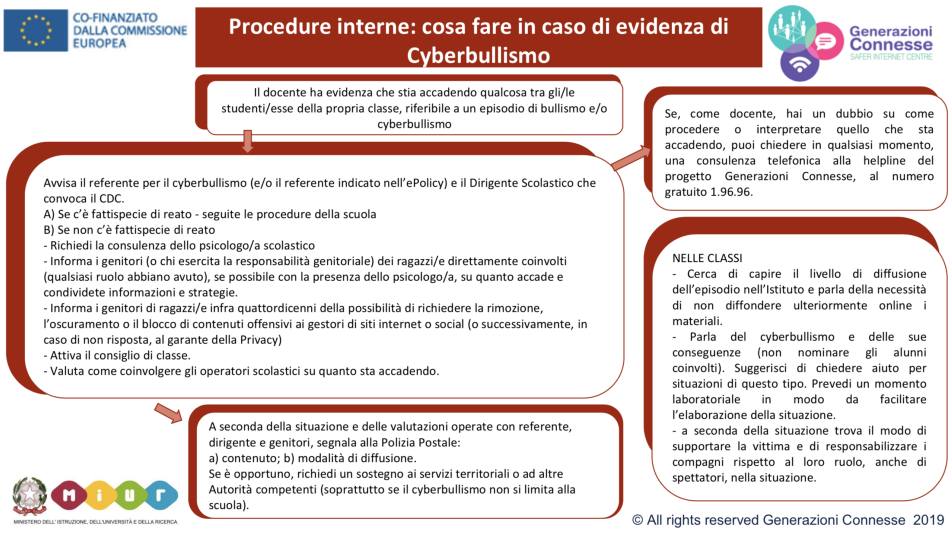
- **Comitato Regionale Unicef**: laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni)**: svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare 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

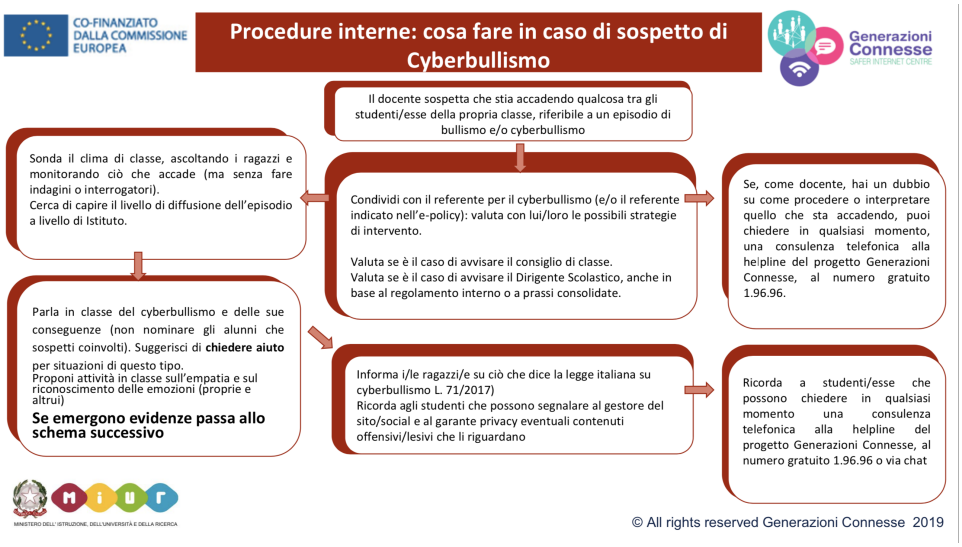
specificatamente rivolti alle dipendenze da Internet e alle situazioni di rischio correlate.

- **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.

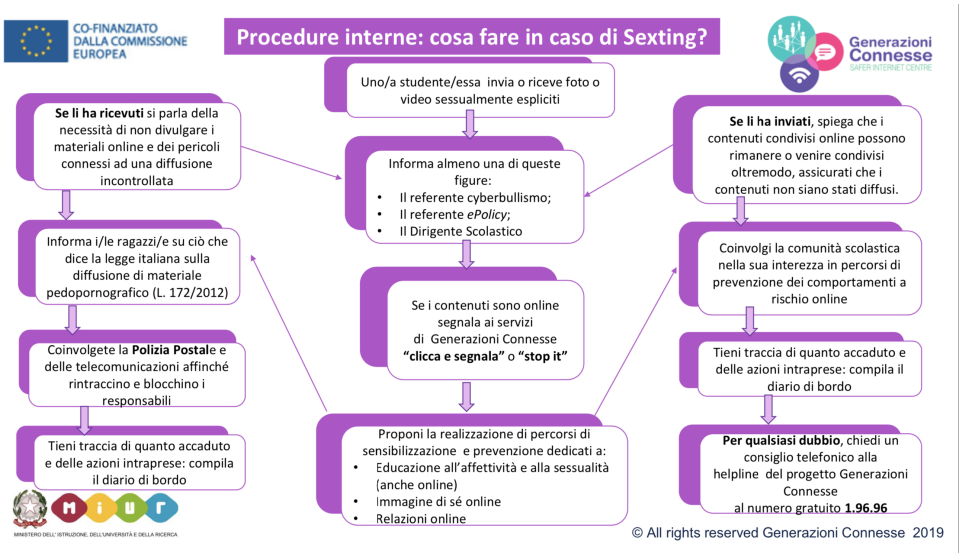
5.4. - Allegati con le procedure

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

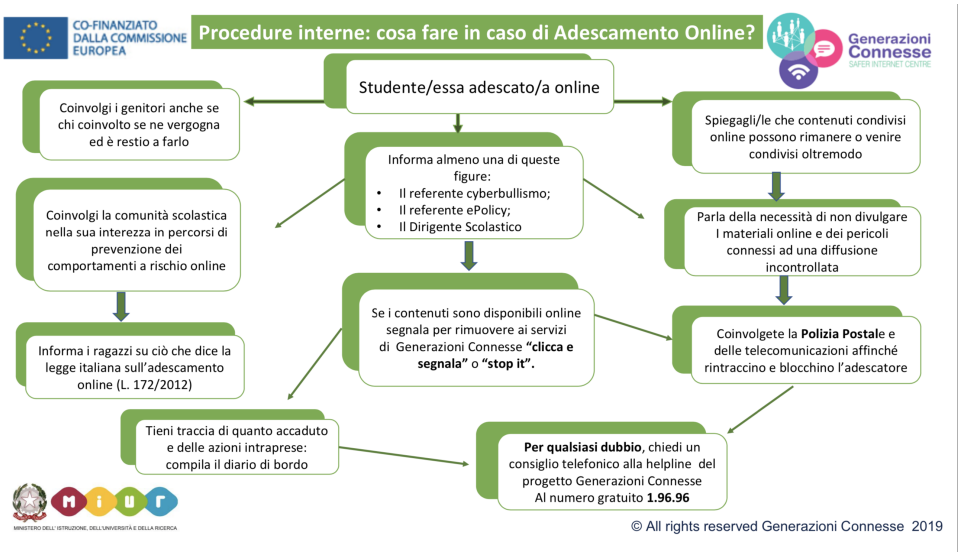




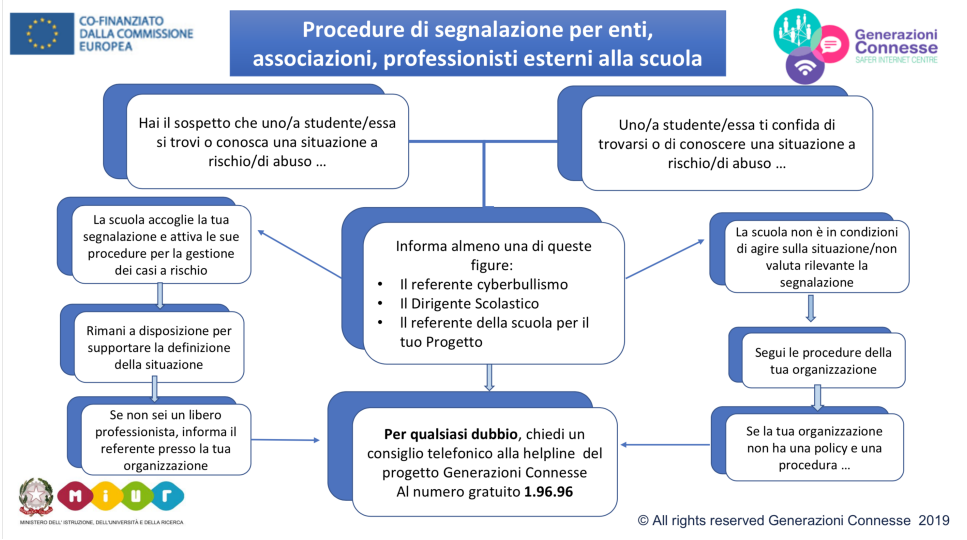
Procedure interne: cosa fare in caso di sexting?



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.

SALVINA GEMMELLARO
29.11.2021 13:23:17 UTC