Documento di ePolicy

CTIC893008

IC G.B. NICOLOSI - PATERNO'

VIA SCALA VECCHIA - 95047 - PATERNO' - CATANIA (CT)

Davide Platania

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" si rivolge a tutte le componenti della Comunità scolastica: il personale della scuola, gli alunni e le famiglie.

L'Istituto Comprensivo "G.B. Nicolosi" di Paternò ha redatto nell'a.s. 2021/2022 la presente e-Policy 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 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.

Nell'ambito di questa ePolicy vengono individuati i seguenti ruoli e le principali responsabilità correlate:

IL DIRIGENTE SCOLASTICO

- è garante della sicurezza, anche online, di tutti i membri della comunità scolastica;
- promuove la cultura della sicurezza online in collaborazione con il Referente di Istituto per il bullismo /cyberbullismo e con il Team Antibullismo;
- promuove percorsi di formazione sulla sicurezza in rete e sulle problematiche

connesse all'utilizzo delle nuiove tecnologie sia in modalità online che offline;
- garantisce l'esistenza di un sistema/protocollo per il monitoraggio e il controlllo interno della sicurezza online;
- gestisce e interviene nei casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali da parte degli studenti e delle studentesse.

L'ANIMATORE DIGITALE

- supporta il personale scolastico da un punto di vista non solo tecnico-informatico, ma anche in riferimento ai rischi online, alla protezione e alla gestione dei dati personali;
- promuove percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale";
- monitora e rileva eventuali episodi o problematiche connesse all'uso delle TIC a scuola.

IL REFERENTE BULLISMO E CYBERBULLISMO

- coordina e promuove iniziative specifiche per la prevenzione e il contrasto del bullismo e cyberbullismo, avvalendosi anche delle Forze di Polizia, delle associazioni, degli enti territoriali e di esperti.

I DOCENTI

- integrano parti del curricolo disciplinare con approfondimenti sull'uso responsabile delle TIC e della RETE servendosi delle tecnologie digitali nella didattica;
- promuono lo sviluppo delle competenze digitali degli allievi facendo sì che gli stessi conoscano e seguano le norme di sicurezza nell'utilizzo del web;
- segnalano alle famiglie eventuali problematiche emerse in classe nell'utilizzo del digitale e stabiliscono linee comuni di intenvento educativo;
- segnalano al Dirigente scolastico e ai suoi collaboratori qualunque violazione, anche online, del Regolamento di Istituto secondo la procedura stabilita.

IL PERSONALE ATA

- svolge funzioni di tipo amministrativo, contabile, gestionale e di sorveglianza, connesse alle attività dell'Istituzione scolastica, in collaborazione con il Dirigente scolastico e con il personale docente tutto;
- segnala al Dirigente scolastico e ai suoi collaboratori comportamenti non adeguati e/o episodi di bullismo/cyberbullismo;
- collabora nel reperire, verificare e valutare informazioni inerenti possibili casi di bullismo/cyberbullismo.

STUDENTI E STUDENTESSE

- rispettano le norme che disciplinano l'uso corretto e responsabile delle tecnologie digitali, come indicato nel Regolamento di Istituto

- adottano le regole di e-safety per evitare situazioni di rischio per sè e per gli altri.

I GENITORI

- partecipano alle iniziative di sensibilizzazione e formazione organizzate dall'Istituto sull'uso consapevole delle TIC e della RETE, nonchè sull'uso responsabile dei device personali;
- condividono con i docenti le linee educative relative alle TIC e alla RETE, al Regolamento di Istituto e al patto di corresponsabilità educativa;
- accettano e condividono il documento di ePolicy dell'Istituto;
- collaborano con la scuola per la prevenzione dei rischi e per l'attuazione delle procedure previste in caso di violazione delle regole stabilite.

GLI ENTI EDUCATIVI ESTERNI E LE ASSOCIAZIONI

- osservano le politiche interne sull'uso consapevole della Rete e delle TIC;
- attivano procedure e comportamenti sicuri per la protezione degli studenti e delle studentesse durante le attività che vengono svolte all'interno della scuola o in cui sono impegnati gli stessi.

Per quanto non espressamente indicato sui ruoli e sulle responsabilità delle figure presenti all'interno dell'Istituzione scolastica, si rimanda: all'art. 21, comma 8, Legge 15 marzo 1997, n. 59; all'art. 25 della Legge 30 marzo 2001, n. 165; al CCNL in vigore; al D.P.R. 8 marzo 1999, n. 275; alla Legge 13 luglio 2015, n. 107; al Piano Nazionale Scuola Digitale; a quanto stabilito in materia di culpa in vigilando, culpa in organizzando, culpa in educando.

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).

Le attività progettuali o di formazione a carattere seminariale, nonchè i contenuti oggetto dell'azione proposta, devono essere preventivamente autorizzate dal Dirigente scolastico, con modalità e tempi concordati.

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 "G.B. Nicolosi" di Paternò insieme ai regolamenti correlati e al Patto di Corresponsabilità.

Tutta la comunità scolastica sarà informata che l'uso di internet e di ogni dispositivo

digitale verrà monitorato dai docenti e che la relativa fruzione potrà avvenire solo con la loro autorizzazione e supervisione.

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 ICT 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 tecnologiue 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.

Il monitoraggio e l'aggiornamento del documento di e-Policy saranno curati dal docente Referente di Istituto per la prevenzione e il contrasto del bullismo e cyberbullismo (che coordinerà l'attività), dal Team antibullismo e dall'Animatore

digitale.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

- Presentazione e conoscenza dell'ePolicy rivolto ai docenti
- Campagna di disseminazione dell'ePolicy rivolta a studenti e genitori

Azioni da svolgere nei prossimi 3 anni:

- Presentazione e conoscenza del progetto Generazioni Connesse rivolto ai docenti
- Organizzare 1 evento di presentazione e attuazione del progetto Generazioni Connesse rivolto agli studenti 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.

Nella stesura del Curricolo Digitale si farà riferimento alle indicazioni presenti nei seguenti documenti:
- Raccomandazione del Consiglio europeo relativa alle competenze chiave per l'apprendimento permanente (C189/9,p9)
- Piano Nazionale Scuola Digitale (PNSD) con particolare riferimento al paragrafo 4.2. su "Competenze e contenuti"
- DigComp 2.1 con 8 livelli di padronanza ed esempi di utilizzo.

Il DigComp, in particolare, è diventato un riferimento per lo sviluppo e la pianificazione strategica di iniziative sulle competenze digitali, sia a livello europeo sia nei singoli stati membri dell'Unione.

Il documento prevede:

- aree di competenze individuate come facenti parte delle competenze digitali;

- descrittori delle competenze e titoli pertinenti a ciascuna area (21 competenze);

- livelli di padronanza per ciascuna competenza (i livelli sono 8);

- conoscenze, abilità ed attitudini applicabili a ciascuna competenza;

- esempi di utilizzo sull'applicabilità della competenza per diversi scopi.

Le aree di competenza individuate dal Digcomp sono nello specifico:

Area 1: "Alfabetizzazione e dati": nello specifico, per quest'area si dovrebbe puntare a sviluppare in bambini e ragazzi le seguenti competenze: navigare, ricercare e filtrare dati, informazioni e contenuti digitali; valutare e gestire dati, informazioni e contenuti digitali; saper riconoscere e sapersi difendere da contenuti dannosi e pericolosi in Rete (es. app, giochi online, siti non adatti ai minori, materiale pornografico e pedo-pornografico ecc.).

Area 2: "Comunicazione e collaborazione" quest'area fa riferimento a sei punti specifici: saper interagire con gli altri attraverso le tecnologie digitali; essere consapevoli nella condivisione delle informazioni in Rete; essere buoni "cittadini digitali"; collaborare adeguatamente con gli altri attraverso le tecnologie digitali; conoscere le "Netiquette", ovvero le norme di comportamento online; saper gestire la propria "identità digitale".

Area 3: "Creazione di contenuti digitali": le specifiche competenze digitali che andranno sviluppate in questo caso sono: creare e modificare contenuti digitali in diversi formati per esprimersi attraverso mezzi digitali; modificare, affinare, migliorare e integrare informazioni e contenuti all'interno di un corpus di conoscenze esistente per creare conoscenze e contenuti nuovi, originali e rilevanti; Capire come il copyright e le licenze si applicano ai dati, alle informazioni e ai contenuti digitali.

Area 4: "Sicurezza": nello specifico, bisognerebbe puntare a sviluppare in bambini e ragazzi le seguenti competenze: imparare a proteggere i dispositivi e i contenuti digitali e comprendere i rischi e le minacce presenti negli ambienti digitali; conoscere le misure di sicurezza e protezione e tenere in debita considerazione l'affidabilità e la privacy; proteggere i dati personali e la privacy negli ambienti digitali, capire come utilizzare e condividere informazioni personali proteggendo se stessi e gli altri dai danni; esercitare i propri diritti in termini di privacy e sicurezza.

In materia di sicurezza in rete, è opportuno riportare qui di seguito il Regolamento per la Didattica Digitale Integrata vigente nel nostro Istituto.

Quanto agli altri Regolamenti adottati dall'I.C.S. "G.B. Nicolosi" di Paternò, unitamente al Curricolo Verticale e ad ogni altro documento di rilevanza, essi possono essere facilmente reperiti all'interno del sito web della scuola

Link al Regolamento per Didattica Digitale Integrata dell'I.C.S. "G.B. Nicolosi" di Paternò:

https://www.gbnicolosi.edu.it/attachments/article/265/Regolamento%20per%20la%20DDI.pdf

---

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

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

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

La competenza digitale, oggi, è imprescindibile per i docenti così come per studenti e studentesse e permette di integrare la didattica con strumenti che la diversificano, la rendono innovativa e in grado di venire incontro ai nuovi stili di apprendimento. I docenti, dunque, devono essere pronti a cogliere questa sfida anche grazie alla possibilità di formazione permanente offerta loro innanzitutto dall'Istituto scolastico, in modo da rispondere ai diversi bisogni formativi della classe.

L'Istituto "G.B. Nicolosi" di Paternò favorisce la partecipazione del personale sia ad iniziative promosse direttamente dalla scuola (ad es. con il supporto dell'Animatore Digitale), dalle reti di scuole e dall'Amministrazione, sia a percorsi formativi liberamente scelti dai docenti (anche online), purché coerenti con il piano di formazione.

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

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

Sul sito web www.gbnicolosi.edu.it è predisposta una sezione dedicata ai docenti in cui essi potranno condividere e consultare materiale informativo sulla sicurezza in internet per l'approfondimento personale, per le attività con gli studenti e per gli incontri con i genitori, costituiti da guide in pdf, video e link messi a disposizione in modo particolare dal sito www.generazioniconnesse.it con il contributo della Polizia di Stato, dei Carabinieri, del Telefono Azzurro, Save the Children e di altri enti o associazioni competenti in materia.

La formazione degli insegnanti è formulata tenuto conto di un'analisi del fabbisogno formativo del corpo docente e degli studenti sull'utilizzo ed integrazione delle TIC nella didattica.

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.

Gli studenti e le studentesse devono attenersi a quanto previsto dai Regolamenti scolastici e dalle Circolari interne emanate dal Dirigente scolastico, sulla base delle

note ministeriali sull'utilizzo consapevole delle tecnologie digitali all'interno del contesto scolastico.

I genitori, nell'azione di corresponsabilità didattico-educativa, rappresentano un punto di forza per l'implementazione dei rapporti "scuola-famiglia", quale garanzia e rispetto degli impegni, di natura anche pedagogica, sottoscritti e condivisi nello stesso Patto di corresponsabilità.

Il nostro Istituto si propone di:
- prevedere strategie per il coinvolgimento delle famiglie in percorsi di sensibilizzazione e formazione all'uso consapevole e costruttivo delle TIC;
- condividere regole sull'uso delle tecnologie digitali da parte della comunità scolastica nella comunicazione con la scuola;
- fornire consigli/linee guida sull'uso delle tecnologie digitali nella comunicazione con i figli e in famiglia (facendo riferimento alla sezione di www.generazioniconnesse.it dedicata ai genitori consultabile sul sito web della scuola).

Il nostro piano d'azioni

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

- Effettuare un'analisi del fabbisogno formativo su studenti e studentesse in relazione alle competenze digitali.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo delle nuove tecnologie nella didattica e sull'utilizzo consapevole e responsabile delle tecnologie digitali.
- Organizzare per i genitori e gli studenti incontri formativi di base sui rischi e sulle opportunità delle nuove tecnologie.
- Organizzare per il corpo docente incontri formativi di base sull'uso delle nuove tecnologie in ambito didattico e sull'utilizzo consapevole e responsabile delle tecnologie digitali.

AZIONI (da sviluppare nell'arco dei tre anni scolastici 2022/2025)

- Organizzare incontri con esperti per i genitori e gli studenti sull'educazione alla cittadinanza digitale.
- Organizzare e promuovere per il corpo docente incontri formativi di approfondimento sull'uso delle nuove tecnologie in ambito didattico e sull'utilizzo consapevole e responsabile delle tecnologie digitali.

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

3.1 - Protezione dei dati personali

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

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

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

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

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

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

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

In merito alla protezione dei dati personali, si fa riferimento a quanto previsto dal Decreto Legislativo del 30 giugno 2003, n.196 (Codice della Privacy), integrato dal D. Lgs. 10 agosto 2018, n. 101, e dal GDPR (General Data Protection Regulation) n. 679 del 2016.

L'Istituto fornisce al personale scolastico, alle famiglie e ai soggetti esterni che a vario titolo devono sottoporre i propri dati personali, un'apposita informativa che esplicita i criteri e le modalità con cui l'informazione viene trattata per le sole finalità correlate all'attività amministrativa oggetto del trattamento.
Nell'ambito scolastico sono molteplici i contesti in cui si rende necessario dare l'informativa di trattamento all'utente: iscrizione a scuola, svolgimento di attività amministrativa della segreteria, partecipazione a corsi di formazione come corsista o esperto, partecipazione a concorsi o manifestazioni, utilizzo di piattaforme informatiche digitali per la didattica a distanza, utilizzo di alcuni servizi dedicati nel sito web d'Istituto.
Le procedure correlate al trattamento e alla conservazione dei dati sono curate dal Data Protect Office (DPO) dell'Istituto che collabora con il Dirigente Scolastico, con l'amministratore di rete, con il personale di segreteria e con i docenti (anch'essi responsabili di trattamento dei dati, per quanto riguarda gli alunni) affinché l'informazione venga veicolata e trattata conformemente ai requisiti del GDPR.
Il personale scolastico coinvolto nel trattamento dei dati è formato adeguatamente tramite incontri periodici con il DPO e con i responsabili della gestione della rete Intranet ed Internet dell'Istituto.
Per quanto concerne l'uso di fotografie, video o altri materiali audiovisivi che ritraggono gli alunni nell'ambito delle attività educative e didattiche per scopi documentativi, formativi e informativi, viene richiesto ai genitori di formalizzare il proprio esplicito consenso alla pubblicazione dei materiali all'interno della Google Workspace (Classroom) con accesso riservato ai genitori del gruppo classe, o, in casi eccezionali, sul sito web dell'Istituto per documentare attività didattiche che si svolgono all'interno della scuola.

L'autorizzazione non consente l'uso dell'immagine in contesti che pregiudichino la propria dignità personale ed il decoro e comunque per uso e/o fini diversi da quelli sopra indicati.

Le autorizzazioni al trattamento dei dati personali vengono annotate nell'apposito registro consensi previsto nel GDPR. La formula utilizzata dalla nostra scuola per richiedere il consenso è semplice e comprensibile.

L'Istituto si impegna non solo a tutelare la privacy degli/lle studenti/esse e delle loro famiglie, ma anche ad informare e soprattutto a rendere consapevoli, di quanto sia importante tutelare il diritto alla riservatezza di se stessi e degli altri.

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.

Di fronte all'emergenza nazionale legata alla diffusione del Covid-19, le tecnologie si sono rivelate improvvisamente un'opportunità per la Scuola, sia in termini didattici sia con riferimento alla gestione amministrativa degli istituti, ma hanno anche mostrato carenze e difficoltà (tecnologiche e di competenze) che hanno messo in evidenza e in taluni casi accentuato le distanze sociali esistenti. Si sono infatti, da subito, evidenziate tra gli studenti disparità di accesso alla connessione internet e disparità di accesso ai device. In questo contesto, allo scopo di garantire il diritto all'istruzione di ciascun alunno, il nostro istituto si è mobilitato tempestivamente, offrendo in comodato d'uso gratuito i dispositivi tecnologici indispensabili per una piena accessibilità alle attività didattiche a distanza.

La scuola garantisce inoltre, previa abilitazione sia dei dispositivi in dotazione della scuola che di quelli personali dei docenti, l'accesso alla rete in ciascuno dei tre plessi dell'Istituto.

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 www.gbnicolosi.edu.it
- registro elettronico Argo
- piattaforma Google Workspace for Education
- canale Telegram rivolto al personale
- un canale Telegram rivolto alle famiglie
- posta elettronica

Sito web istituzionale

Il sito della scuola nasce per una corretta organizzazione delle informazioni istituzionali. Esso viene costantemente aggiornato affinchè tutti gli utenti esterni ed interni della scuola (famiglie, alunni, docenti, territorio) siano tempestivamente informati sulle attività e iniziative svolte, sui contenuti didattici ed educativi e sull'organizzazione della scuola.

Il personale dell'Istituto, previa autenticazione attraverso credenziali individuali, accede all'area riservata del sito web istituzionale per fruire di materiale didattico-organizzativo ad esso dedicato e per la consultazione di circolari e comunicazioni interne.

Registro elettronico

Il registro elettronico Argo in adozione dall'Istituto è uno strumento che, nel rispetto della normativa vigente, permette un'interazione in tempo reale tra la scuola e la famiglia, oltre ad offrire al personale interno servizi per la gestione delle proprie richieste. La sicurezza e la privacy sono controllate attraverso credenziali d'accesso individuali, generate da un'apposita procedura interna e comunicate direttamente agli interessati. Si possono verificare in tempo reale i risultati scolastici dei propri figli, le assenze, i ritardi ed eventuali procedimenti disciplinari. Si possono verificare, inoltre, i compiti assegnati, gli argomenti trattati durante le lezioni e le valutazioni.

Piattaforma Google Workspace for Education

La piattaforma Google Workspace for Education consiste in una suite di applicazioni gratuite ideata da Google allo scopo di sostenere l'innovazione del sistema scolastico, favorendo la semplificazione delle attività amministrative della scuola e promuovendo la creazione di ambienti di apprendimento accattivanti, dinamici ed efficaci.

In particolare, Google Classroom è uno strumento che, garantendo standard di sicurezza elevati, permette agli insegnanti di creare classi virtuali attraverso cui è possibile comunicare con gli studenti, promuovere attività collaborative, assegnare compiti e valutarli, monitorare i progressi, inviare feedback e organizzare efficacemente risorse didattiche e materiali.

Google Workspace for Education è una piattaforma che consente una continuità trasversale tra i diversi ordini di scuola.

Telegram

Telegram è un'app di messaggistica istantanea che consente di inviare messaggi, comunicazioni, informazioni in maniera rapida e immediata. La scuola, attraverso Telegram, ha predisposto due canali: il primo permette al Dirigente scolastico e ai suoi collaboratori di inviare comunicazioni importanti al personale scolastico, mentre il secondo è rivolto all'utenza.

Posta elettronica

La comunicazione istituzionale avviene attraverso posta elettronica ordinaria (PEO) oppure tramite posta elttronica certificata (PEC):

- ctic893008@istruzione.it (PEO)

- ctic893008@pec.istruzione.it (PEC)

Nell'ambito degli account Google Workspace for Education, i docenti, il personale ATA e gli studenti, accedendo attraverso le proprie credenziali, fruiscono inoltre di un servizio di posta elettronica con dominio @gbnicolosi.edu.it.

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.

All'interno del PNSD, pilastro fondamentale de La buona scuola (L.107/2015) è prevista una specifica azione che incentiva l'utilizzo didattico dei dispositivi personali dei docenti e degli alunni. L'azione #6 del PNSD (Linee Guida per politiche attive di Byod - Bring Your Own Device) favorisce inoltre l'integrazione di tali dispositivi personali con le dotazioni tecnologiche della scuola.

In questo contesto, pur mantenendo il divieto di utilizzo non autorizzato di smartphone e tablet da parte degli alunni, è consentito il ricorso a fini esclusivamente didattici di tali dispositivi personali, favorendo una didattica di tipo laboratoriale, più vicina ai nuovi modi di comunicare, di socializzare e di apprendere, e promuovendo lo sviluppo di competenze di cittadinanza digitale.

Il nostro piano d'azioni

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

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli studenti e del personale scolastico.
- Organizzare uno o più eventi volti a formare gli studenti e il personale scolastico sui temi delle tecnologie digitali, della protezione dei dati personali e dell'uso consapevole, sicuro e responsabile di internet e dei social media.

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

- Organizzare uno o più eventi volti a garantire che almeno l'80% della comunità scolastica raggiunga adeguate competenze sui temi delle tecnologie digitali, della protezione dei dati personali e dell'uso consapevole, sicuro e responsabile di internet e dei social media.

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, 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 nella secondaria di primo grado, per gli interventi di "prevenzione universale" (rivolta a tutti quando non si è riscontrato nessun problema specifico), l'istituto "G.B. Nicolosi" di Paternò 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 o, a seconda del caso, nelle modalità indicate dal "Protocollo di gestione delle Emergenze" (in corso di elaborazione) 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.

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).

Chi compie atti di cyberbullismo può rendersi responsabile di reati penali e danni civili (diffamazione, violenza privata, minacce, ingiuria, ecc.). La responsabilità penale è personale e l'imputabilità penale scatta al 14° anno di età se la persona è in grado di intendere e di volere. La responsabilità civile, per i minori di 14 anni ricade sui genitori (se si verifica "culpa in educando"), sugli insegnanti e sul dirigente (se si verifica "culpa in vigilando" e/o "culpa in organizzando").

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.

Il nostro Istituto si impegna a lavorare alla decostruzione di stereotipi con approccio curricolare e attraverso la partecipazione a bandi e progetti.

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 nostra scuola si impegna a:

- attivare una indagine su una eventuale dipendenza da internet e dal gioco online;

- lavorare sul tema dell'adolescenza (anche con approccio curricolare) e attivare percorsi di approfondimento al fine di 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' I.C.S. "G.B. Nicolosi" di Paternò intende accompagnare ragazze e ragazzi in un percorso di educazione (anche digitale) all'affettività e alla sessualità, attraverso l'approfondimento, anche in chiave curriculare, dei temi dell'affettività, del digitale e della sessualità, 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.

Nel momento in cui viene ricevuta la segnalazione, gli operatori procederanno a coinvolgere le autorità competenti in materia, con l'obiettivo di facilitare il processo di rimozione del materiale stesso dalla Rete e allo stesso tempo consentire le opportune attività investigative, finalizzate ad identificare chi si trova in possesso di quel materiale, chi lo diffonde e chi lo produce, ma, soprattutto, ad identificare i minori abusati presenti nelle immagini e video, fermando l'abuso che potrebbe essere ancora in corso e attivando il necessario supporto per la vittima.
Inoltre, se si riscontra un rischio per il benessere psicofisico dei bambini o dei ragazzi coinvolti nella visione di questi contenuti sarà opportuno ricorrere a un supporto psicologico. Le strutture pubbliche a cui rivolgersi sono i servizi socio-sanitari del territorio di Paternò: Consultorio Familiare, Servizi di Neuropsichiatria infantile, centri specializzati sull'abuso e il maltrattamento all'infanzia, etc.
Qualora si venisse a conoscenza di tale tipologia di reato sarà possibile far riferimento alla Polizia di Stato – Compartimento di Polizia postale e delle Comunicazioni, alla Polizia di Stato – Questura o Commissariato di P.S., all'Arma dei Carabinieri – Comando Provinciale o Stazione di Paternò; alla Polizia di Stato – Commissariato online.

Il nostro piano d'azioni

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

- Promuovere la riflessione personale e il dibattito in classe con gli alunni

sui temi del sexting, dell'hating, della dipendenza da gioco e dell'adescamento online.

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

- Promuovere la riflessione personale e il dibattito in classe con gli alunni sui temi del sexting, dell'hating, della dipendenza da gioco e dell'adescamento online.

- Organizzare uno o più incontri di sensibilizzazione con esperti sui rischi online e sull'utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti, ai genitori e ai docenti.

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.

Si ritiene che debbano essere segnalate tutte quelle situazioni caratterizzate da volontarie e ripetute aggressioni mirate a offendere, minacciare, diffamare e/o ferire una persona (o un piccolo gruppo) tramite un utilizzo irresponsabile di internet.

L' I.C. "G.B.Nicolosi"di Paternò, quindi, 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 e al sexting.

E' importante sottolineare che nella maggior parte dei succitati fenomeni, il rischio non è correlato tanto all'uso improprio delle ICT quanto al contenuto semantico delle informazioni che attraverso la rete si diffondono. Pertanto, gli strumenti digitali di monitoraggio potrebbero rivelarsi inefficaci nella prevenzione e nel contrasto di questa tipologia di rischio.
Per questo motivo sarà cura dei docenti, in collaborazione con i genitori, monitorare l'attività digitale dei singoli gruppi classe e segnalare al team di prevenzione eventuali episodi di scambi di contenuti impropri:
- contenuti afferenti la violazione della privacy (foto personali, l'indirizzo di casa o il telefono, informazioni private proprie o di amici, foto o video pubblicati contro la propria volontà, eventi privati, ecc.);
- contenuti afferenti all'aggressività o alla violenza (messaggi minacciosi, commenti offensivi, pettegolezzi, informazioni false, foto o video imbarazzanti, virus, contenuti razzisti, che inneggiano al suicidio, immagini o video umilianti, insulti, videogiochi pensati per un pubblico adulto, ecc.);
- contenuti afferenti alla sessualità: messaggi molesti, conversazioni (testo o voce) che connotano una relazione intima, foto o video personali con nudità o abbigliamento succinto, immagini pornografiche, foto e video in cui persone di minore età sono coinvolte o assistono ad attività sessuali (pedopornografia), ecc.
Tutte le segnalazioni riportate dai docenti verranno registrate attraverso un'apposita scheda secondo il protocollo d'intervento.

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.

In relazione al CASO A, è opportuno il coinvolgimento del Referente d'Istituto per il contrasto del bullismo e del cyberbullismo, al fine di valutare le possibili strategie d'intervento. Se si ravvisano gli estremi, viene informato il Dirigente scolastico unitamente al Consiglio di classe. Uno strumento utile per raccogliere informazioni può essere il diario di bordo (allegato alla presente e-Policy): il docente deve cercare di capire se gli episodi sono circoscritti al gruppo o interessano l'intero Istituto. E' fondamentale coinvolgere tutti gli studenti e le studentesse, informandoli sui fenomeni e sulle caratteristiche degli stessi e suggerendo di chiedere aiuto qualora ritenessero di essere coinvolti da fenomeni di bullismo, cyberbullismo o sexting.

In relazione al CASO B, il docente deve condividere immediatamente quanto osservato

con il Referente per il bullismo e il cyberbullismo, al fine di valutare insieme le possibili strategie di intervento. Si avvisa anche il Dirigente Scolastico che convoca il Consiglio di classe. Se non si ravvisano fattispecie di reato, è opportuno: informare i genitori (o chi esercita la responsabilità genitoriale) degli/delle studenti/studentesse direttamente coinvolti/e (qualsiasi ruolo abbiano avuto), se possibile con la presenza di professionisti, per attivare strategie condivise e modalità di supporto, creare momenti di confronto costruttivo in classe, con la presenza di figure specialistiche territoriali, informare i genitori degli/delle studenti/studentesse sotto i quattordici anni della possibilità di richiedere la rimozione, l'oscuramento o il blocco di contenuti offensivi ai gestori di siti internet o social (o successivamente, in caso di non risposta, al garante della Privacy), informare gli/le studenti/studentesse ultra quattordicenni della possibilità di richiedere la rimozione, l'oscuramento o il blocco di contenuti offensivi ai gestori di siti internet o Social (o successivamente, in caso di non risposta, al garante della Privacy), convocare il consiglio di classe, valutare come coinvolgere gli operatori scolastici su quello che sta accadendo.

A seconda della situazione e delle valutazioni effettuate con il Referente, il Dirigente e i genitori, sarebbe inoltre opportuno segnalare alla Polizia Postale, ove necessario, ai sensi di legge:

a. contenuto offensivo del materiale online;

b. modalità di diffusione;

c. eventuale fattispecie di reato.

Qualora si ritenesse opportuno, l'Istituto richiederà un sostegno ai servizi e alle associazioni territoriali o ad altre autorità competenti.

E' bene sempre dialogare con la classe, attraverso interventi educativi specifici, cercando di sensibilizzare studenti e studentesse sulla necessità di non diffondere ulteriormente online i materiali dannosi e suggerendo piuttosto di segnalarli e bloccarli.

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.

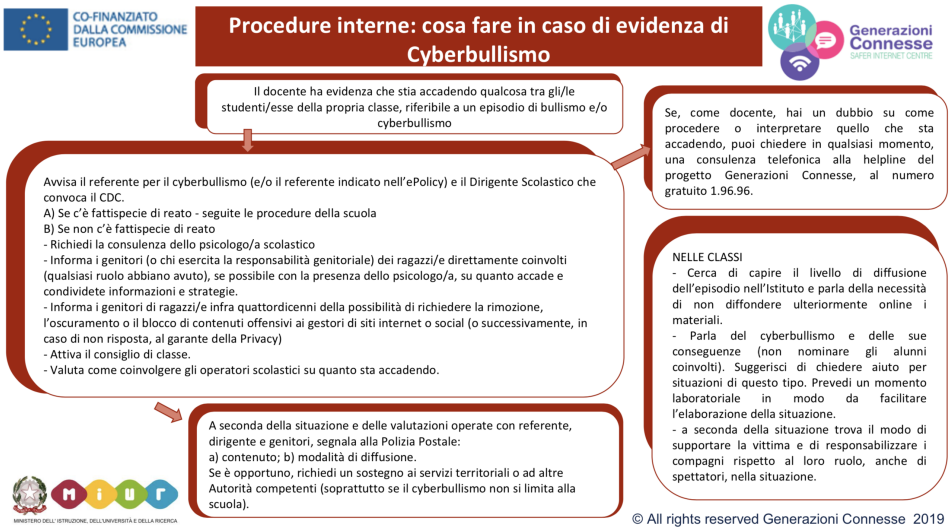
A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all'utilizzo di Internet può presentare.

- **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.

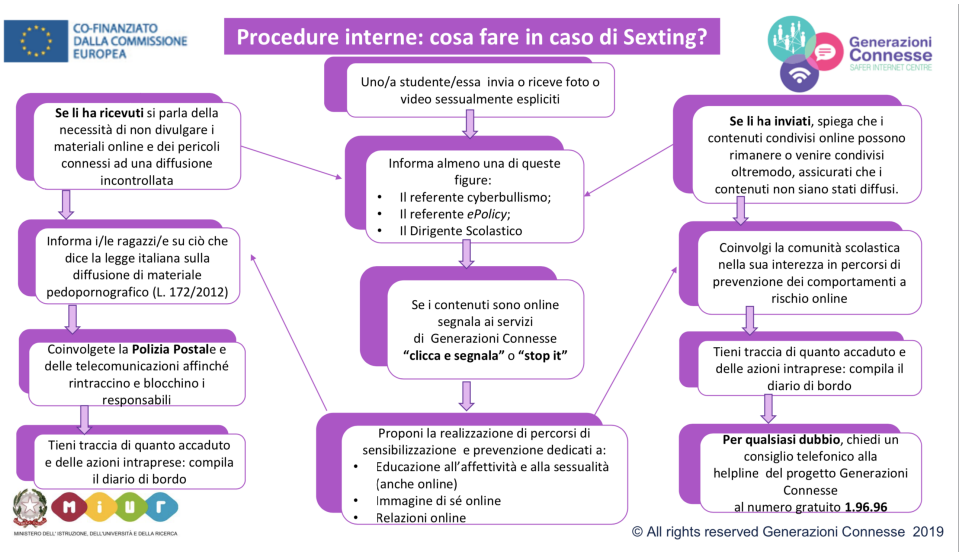
Attualmente nel nostro Istituto esistono prassi informali di comunicazione con le autorità competenti e con i servizi socio-sanitari del territorio per la gestione condivisa di episodi e/o comportamenti a rischio associati all'utilizzo delle tecnologie digitali.

5.4. - Allegati con le procedure

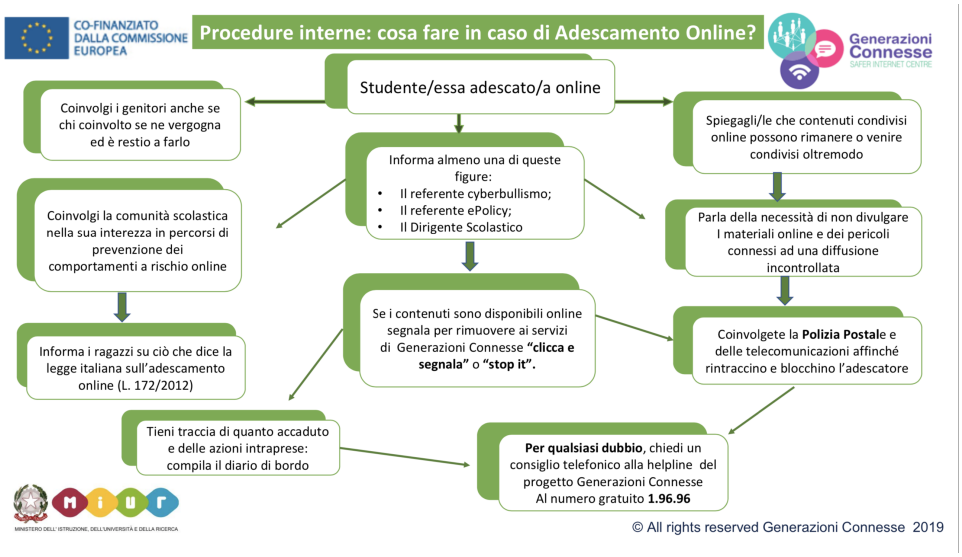
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



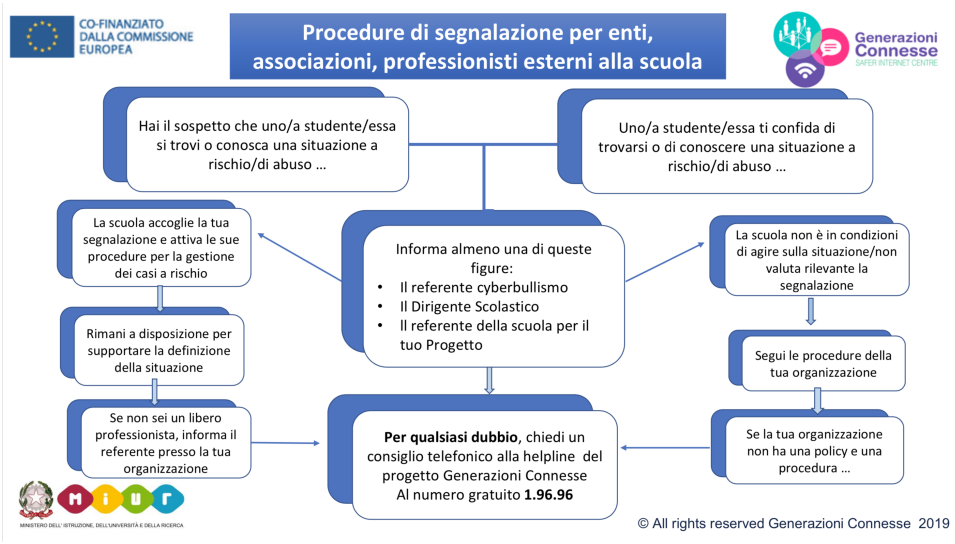
Procedure interne: cosa fare in caso di sexting?



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

Il nostro piano d'azioni

IL NOSTRO PIANO DI 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 e studentesse, 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;

- promozione dell'Educazione Civica Digitale.