

IC - "S. SCANDURA" - ACICATENA
Prot. 0007219 del 26/09/2022
II-11 (Uscita)



Documento di ePolicy

CTIC814007

IC SCANDURA ACI CATENA

VIA DR. CHIARENZA - 95022 - ACI CATENA - CATANIA (CT)

Roberto Maniscalco

Capitolo 1 - Introduzione al documento di ePolicy

1.1 - Scopo dell'ePolicy

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

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

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

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

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

Argomenti del Documento

1. Presentazione dell'ePolicy

1. Scopo dell'ePolicy
2. Ruoli e responsabilità
3. Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto
4. Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica
5. Gestione delle infrazioni alla ePolicy
6. Integrazione dell'ePolicy con regolamenti esistenti
7. Monitoraggio dell'implementazione dell'ePolicy e suo aggiornamento

2. Formazione e curriculum

1. Curriculum sulle competenze digitali per gli studenti
2. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica
3. Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali
4. Sensibilizzazione delle famiglie e Patto di corresponsabilità

3. Gestione dell'infrastruttura e della strumentazione ICT (Information and Communication Technology) della e nella scuola

1. Protezione dei dati personali
2. Accesso ad Internet
3. Strumenti di comunicazione online
4. Strumentazione personale

4. Rischi on line: conoscere, prevenire e rilevare

1. Sensibilizzazione e prevenzione
2. Cyberbullismo: che cos'è e come prevenirlo
3. Hate speech: che cos'è e come prevenirlo
4. Dipendenza da Internet e gioco online
5. Sexting
6. Adescamento online
7. Pedopornografia

5. Segnalazione e gestione dei casi

1. Cosa segnalare
2. Come segnalare: quali strumenti e a chi
3. Gli attori sul territorio per intervenire
4. Allegati con le procedure

Perché è importante dotarsi di una E-policy?

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

all'uso di Internet.

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

Il presente documento mira a descrivere la linea di condotta dell'Istituto comprensivo "**Sebastiano Scandura**" di Aci Catena nei confronti dell'utilizzo delle tecnologie dell'informazione e delle comunicazioni nella didattica, in ambito scolastico ed extra-scolastico, nonché ad educare e sensibilizzare gli adolescenti, gli insegnanti e i genitori all'uso sicuro e consapevole di internet.

Nello specifico il documento mira a promuovere un uso critico da parte degli alunni delle tecnologie digitali e di internet; a far acquisire loro corrette norme comportamentali, procedure e competenze per l'utilizzo delle TIC, a prevenire, rilevare e fronteggiare le problematiche che derivano da un utilizzo non responsabile, pericoloso o dannoso, delle tecnologie digitali.

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.

Il Dirigente scolastico ha il compito di:

- Garantire la sicurezza (tra cui la sicurezza online) di tutti i membri della comunità scolastica.
- Promuovere la cultura della sicurezza online attraverso l'attivazione di corsi di formazione e informazione specifici per tutte le figure scolastiche sull'utilizzo positivo e responsabile delle TIC.
- Garantire l'esistenza di un sistema in grado di consentire il monitoraggio e il controllo interno della sicurezza online.
- Gestire e intervenire in caso di gravi episodi di cyberbullismo e uso improprio delle tecnologie digitali.

L'Animatore digitale, ha il compito di:

- Stimolare la formazione interna all'istituzione sui temi del PNSD (Piano Nazionale Scuola Digitale) e fornire consulenza e informazioni al personale della scuola, agli alunni e alle loro famiglie in relazione ai rischi online e alle misure di prevenzione e gestione degli stessi;
- monitorare e rilevare eventuali episodi o problematiche connesse all'uso delle TIC a scuola, e avere il compito di controllare che gli utenti autorizzati accedano alla Rete della scuola con apposita password, per scopi istituzionali e consentiti (istruzione e formazione);
- Individuare soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola.

Il Referente alla prevenzione del bullismo e del cyberbullismo ha il compito di:

- coordinare e promuovere iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo. A tal fine, può **avvalersi della collaborazione delle Forze di polizia**, delle associazioni e dei centri di aggregazione giovanile del territorio.
- Fondamentale, dunque, il suo ruolo non solo in ambito scolastico ma anche in quello extrascolastico, in quanto (ove possibile) può coinvolgere, con progetti e percorsi formativi ad hoc, studenti, colleghi e genitori.

I Docenti hanno il compito di:

- diffondere la cultura dell'uso responsabile delle TIC e della Rete;
- integrare parti del curriculum della propria disciplina con approfondimenti ad hoc, promuovendo, laddove possibile, anche l'uso delle tecnologie digitali nella didattica;
- accompagnare e supportare gli studenti e le studentesse nelle attività di apprendimento e nei laboratori che prevedono l'uso della LIM o di altri dispositivi tecnologici che si connettono alla Rete;

I Docenti **hanno inoltre il dovere morale e professionale di segnalare al Dirigente Scolastico qualunque problematica, violazione o abuso**, anche online, che vede coinvolti studenti e studentesse.

Il Direttore dei servizi generali amministrativi ha il compito di:

- Garantire, nei limiti delle risorse finanziarie disponibili, che l'infrastruttura tecnica della scuola sia funzionante, sicura e non aperta a uso improprio o a attacchi esterni dannosi o malevoli.

Il Personale ATA

Esiste un **concreto coinvolgimento del personale ATA** nell'applicazione della [legge 107/15 \("La Buona Scuola"\)](#) che concerne non solo il tempo scuola e il potenziamento dell'offerta formativa, ma anche le attività di formazione e autoformazione in tema di bullismo e cyberbullismo.

Il personale ATA qualora dovesse esserne a conoscenza è **coinvolto nel segnalare comportamenti non adeguati e/o episodi di bullismo/cyberbullismo**, insieme ad altre figure e nel raccogliere, verificare e valutare le informazioni inerenti possibili casi di bullismo/cyberbullismo.

Gli Studenti e le Studentesse hanno il compito di:

- in relazione al proprio grado di maturità e consapevolezza raggiunta, utilizzare al meglio le tecnologie digitali in coerenza con quanto richiesto dai docenti;
- con il supporto della scuola devono **imparare a tutelarsi online**, tutelare i/le propri/e compagni/e e rispettarli/le;
- partecipare 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;

I Genitori hanno il compito di:

- in continuità con l'Istituto scolastico, essere partecipi e attivi nelle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete, nonché sull'uso responsabile dei device personali;
- relazionarsi in modo costruttivo con i docenti sulle linee educative che riguardano le TIC e la Rete e comunicare

con loro circa i problemi rilevati quando i/le propri/e figli/e non usano responsabilmente le tecnologie digitali o Internet.

- partecipare ad iniziative di formazione e informazione legate all'uso responsabile delle tecnologie digitali e della Rete;
- **accettare e condividere quanto scritto nell'ePolicy dell'Istituto.**

IMPORTANTE

Si ricorda che esiste una corresponsabilità educativa e formativa che riguarda sia i genitori che la scuola nel percorso di crescita degli studenti e delle studentesse.

In particolare, il 2° comma dell'art. 2048 c.c. così recita: *"I precettori e coloro che insegnano un mestiere o un'arte sono responsabili del danno cagionato dal fatto illecito dei loro allievi e apprendisti nel tempo in cui sono sotto la loro vigilanza"*. Per i genitori, invece, bisogna considerare: il 1° comma dell'art. 30 della Costituzione *"è dovere e diritto dei genitori mantenere, istruire ed educare i figli, anche se nati fuori del matrimonio"*; il 1° comma dell'art. 2048 c.c. ai sensi del quale *"il padre e la madre o il tutore sono responsabili del danno cagionato dal fatto illecito dei figli minori non emancipati o delle persone soggette alla tutela, che abitano con essi (...)"*; l'art. 147 del c.c. *"l'obbligo di mantenere, istruire, educare e assistere moralmente i figli, nel rispetto delle loro capacità, inclinazioni naturali e aspirazioni (...)"*.

Dato questo quadro normativo, rispetto ad un profilo prettamente processuale anche in materia di bullismo e cyberbullismo (dunque non in via esclusiva), si può parlare di **tre tipologie di "culpa"**:

- **culpa in vigilando:** concerne la mancata sorveglianza attiva da parte del docente responsabile verso il minore (così come da art. 2048 del c.c.). Tale condizione è superabile se ci si avvale di una prova liberatoria di non aver potuto impedire il fatto (recita il terzo comma dell'art. 2048 c.c.: *"le persone indicate nei commi precedenti sono liberate dalla responsabilità soltanto se provano di non aver potuto impedire il fatto"*).
- **culpa in organizzando:** si riferisce ai provvedimenti previsti e presi dal Dirigente Scolastico ritenuti come non soddisfacenti e quindi elemento favorevole al verificarsi dell'eventuale incidente.
- **culpa in educando:** fa capo ai genitori i quali hanno instaurato una relazione educativa con il/la figlio/a, ritenuta come non adeguata, insufficiente o comunque carente tale da metterlo/a nella situazione di poter recare danno a terzi.

Gli Enti educativi esterni e le associazioni dovranno:

- conformarsi alla politica della stessa riguardo all'uso consapevole della Rete e delle TIC;
 - promuovere comportamenti sicuri, la sicurezza online e assicurare la protezione degli studenti e delle studentesse durante le attività che si svolgono insieme.
-

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).

Viene prevista la realizzazione di un'informativa sintetica sull'epolicy per i soggetti esterni che erogano attività educative nell'Istituto, con particolare riguardo a procedure di segnalazione di episodi a rischio, che li sensibilizzi e renda consapevoli dei rischi online in cui possono incorrere studenti e studentesse e dei comportamenti corretti da adottare a scuola. E' previsto che in caso di sospetto e/o del verificarsi di episodi che possano mettere in pericolo studenti e studentesse si rivolgano in primis al Dirigente scolastico, ad uno dei suoi diretti

collaboratori ed al Referente del bullismo/cyberbullismo dei quali verranno forniti gli opportuni riferimenti interni per la relativa e tempestiva comunicazione.

I soggetti esterni, prima di lavorare all'interno dell'istituzione scolastica, dovranno firmare per presa visione e accettazione del documento sintetico e-policy .

1.4 - Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica

Il documento di E-policy viene condiviso con tutta la comunità educante, ponendo al centro gli studenti e le studentesse e sottolineando compiti, funzioni e attività reciproche. È molto importante che ciascun attore scolastico (dai docenti agli/le studenti/esse) si faccia a sua volta promotore del documento.

L'E-policy viene condivisa e comunicata al personale, agli studenti e alle studentesse, alla comunità scolastica attraverso:

- la pubblicazione del documento sul sito istituzionale della scuola;
- il Patto di Corresponsabilità, che deve essere sottoscritto dalle famiglie e rilasciato alle stesse all'inizio dell'anno scolastico;

Il documento è approvato dal Collegio dei Docenti e dal Consiglio di Istituto e viene esposto in versione semplificata negli spazi che dispongono di pc collegati alla Rete o comunque esposto in vari punti spaziali dell'Istituto.

Gli studenti e le studentesse vengono informati sul fatto che sono monitorati e supportati nella navigazione on line, negli spazi della scuola e sulle regole di condotta da tenere in Rete.

Nella prima riunione del Collegio Docenti, successiva alla redazione dell'ePolicy, si darà ampia diffusione al redatto documento per dividerlo e trarre spunti utili per il miglioramento. In una successiva riunione del Collegio Docenti se ne curerà l'approvazione da parte dello stesso e del Consiglio di Istituto. Ai coordinatori di classe si fornirà copia dematerializzata del documento per la condivisione con gli studenti e studentesse delle loro classi. Inoltre, se ne curerà l'inserimento sul sito istituzionale della scuola ed espliciti riferimenti all'e-Policy verranno inseriti nel Patto di corresponsabilità, per darne comunicazione alle famiglie.

Sarà redatta una versione child friendly del documento per la comunicazione e la sensibilizzazione ai/lle bambini/e e ai/lle ragazzi/e. Nella comunicazione e condivisione dell'ePolicy è importante, infatti, valutare i vari target di riferimento (studenti/studentesse, docenti, genitori, personale amministrativo, collaboratori scolastici etc.) individuando di conseguenza i linguaggi, le modalità e i canali di comunicazione e condivisione più adatti.

È molto importante, inoltre, sottolineare che ciascun attore scolastico (dai docenti agli/lle studenti/esse) cercherà di farsi a sua volta promotore del documento.

Sintetica informativa sull'ePolicy con relativa procedura di segnalazione verrà fornita ai soggetti esterni che erogano attività educative nell'Istituto.

1.5 - Gestione delle infrazioni alla ePolicy

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

Quando si viene a conoscenza di un atto che potrebbe essere configurabile come cyberbullismo ne consegue l'informazione immediata al Dirigente Scolastico o a uno dei suoi diretti collaboratori o al Referente del Bullismo/CYberbullismo da parte di alunni, di famiglie, di tutto il personale ATA e di qualsiasi altro soggetto che intraprenda attività in ambito scolastico. Il Dirigente Scolastico o il soggetto autorizzato da quest'ultimo, avuta conoscenza del presunto caso di cyberbullismo, informa tempestivamente i soggetti esercenti la responsabilità genitoriale ovvero i tutori dei minori coinvolti e avvia l'istruttoria. Terminata l'istruttoria, se il fatto integra la condotta tipica di cyberbullismo, il DS, in ragione della gravità del caso, convoca il Consiglio di Classe e/o il Consiglio di Istituto allargato ai genitori e/o tutori dei minori coinvolti nonché ai rappresentanti di classe dei genitori con la partecipazione dei servizi socio-assistenziali del territorio, per l'adozione delle sanzioni conseguenti. Qualora gli atti di cyberbullismo si configurino come

veri e propri reati perseguibili d'ufficio il Dirigente Scolastico inoltra tempestiva denuncia all'Autorità Giudiziaria e/o agli Organi competenti.

Nel momento in cui gli alunni faranno un uso improprio delle tecnologie digitali saranno previste le seguenti procedure operative:

Procedure operative per la gestione delle infrazioni alla E-Safety Policy

Infrazioni lievi	Sanzioni	Interventi educativi riparatori	Organo competente
Collegamento a siti web non indicati dai docenti	Richiamo verbale Nota sul diario/libretto personale dell'alunno	Riflessione sul comportamento che l'alunno ha adottato e sulle motivazioni che l'hanno determinate	Insegnante di classe
Utilizzare la rete per interessi privati e personali che esulano dalla didattica	Annotazione sul registro di classe	Richiesta di scuse verbali	
Scaricare file, video-musicali protetti da copyright			
Infrazioni gravi	Sanzioni	Interventi educativi riparatori	Organo competente
Deridere, denigrare, umiliare, calunniare attraverso l'uso delle TIC	Comunicazione scritta alla famiglia. Ammonimento del Dirigente (se reiterate).	Riflessione sul comportamento che l'alunno ha adottato e sulle motivazioni che l'hanno determinato	Insegnante di classe; Dirigente Scolastico o suoi diretti collaboratori;
Divulgare immagini senza il permesso dei soggetti coinvolti.	Convocazione dei genitori.	Richiesta di scuse pubbliche Produzione obbligatoria di un elaborato (da svolgere a casa in collaborazione coi genitori) sui fatti accaduti e riflessioni sulle conseguenze delle proprie azioni.	Responsabile cyberbullismo; Consiglio di classe

Non rispettare le regole d'accesso alle strumentazioni	Richiamo verbale. Annotazione sul registro di classe. Comunicazione scritta alla famiglia.	Riflessione sul comportamento che l'alunno ha adottato e sulle motivazioni che l'hanno determinato	Insegnante di classe Dirigente Scolastico o suoi diretti collaboratori;
Non rispettare le regole d'accesso ad internet	Sequestro temporaneo della strumentazione utilizzata in modo scorretto e restituzione all'alunno al termine della giornata scolastica.	Assegnazione di un lavoro in classe durante i momenti di riposo o a casa	Responsabile cyberbullismo; Animatore digitale
Uso scorretto della strumentazione personale	Sequestro temporaneo della strumentazione utilizzata in modo scorretto e restituzione al genitore al termine della giornata scolastica. Convocazione dei genitori Sospensione dalle lezioni	Assegnazione di un compito di rinforzo, da eseguirsi a casa, inerente l'attività svolta in classe al momento della mancanza disciplinare Studio delle regole di sicurezza non rispettate Studio e ricerca di danni conseguenti a episodi di violazione delle regole e presentazione relazione in classe Svolgimento di mansioni utili alla comunità scolastica	Consiglio di classe Consiglio Istituto
Infrazioni gravissime	Sanzioni	Interventi educativi riparatori	Organo competente
Isolare o emarginare attraverso l'uso delle TIC	Annotazione sul registro di classe. Ammonimento del Dirigente.	Riflessione sul comportamento che l'alunno ha adottato e sulle motivazioni che l'hanno determinate	Insegnante di classe Dirigente Scolastico o suoi diretti collaboratori;
Non rispettare i diritti altrui in ambito di cittadinanza digitale	Convocazione immediata dei genitori.	Produzione obbligatoria di un elaborato (da svolgere a casa in collaborazione coi genitori) sui fatti accaduti e riflessioni sulle conseguenze delle proprie azioni	Responsabile cyberbullismo Consiglio di classe
Minacciare attraverso l'uso delle TIC	Sospensione dalle lezioni.	Conversione della sospensione dalle lezioni con attività socialmente utili favorendo un reale e concreto confronto con i valori della solidarietà e l'assunzione di stili di comportamento positivo, che sviluppino la formazione di una coscienza responsabile e la crescita consapevole dei giovani	Consiglio Istituto Assistenti sociali Forze dell'ordine
Attuare cyberstalking o altre forme di persecuzione e molestia attraverso l'uso delle TIC	Segnalazione agli assistenti sociali (se reiterate).		
Publicare sui social network o inviare tramite messaggistica immagini, video o testi che:	Segnalazione alle autorità competenti in caso di reati.		
- siano offensivi della dignità personale violino le norme della Privacy			
- non siano rispettosi dei valori di uguaglianza e di pari opportunità			
-siano discriminanti (a sfondo etnico, religioso, sessuale...)			
-incoraggino, atteggiamenti di maschilismo o stereotipi di genere			

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.

Verranno inserite nuove norme inerenti l'uso consapevole dei dispositivi informatici e di internet e ne sarà data ampia diffusione a tutti soggetti della scuola: utenti ed operatori interni ed esterni.

ATTENZIONE

I POTETICHE REGOLE CHE POSSIAMO INSERIRE O NON INSERIRE (solo citare come già fatto)

- Ogni allievo è direttamente responsabile della postazione assegnatagli per le ore in cui vi svolge lezione .
- Agli utenti è fatto assoluto divieto di cancellare ,modificare in qualsiasi modo i files presenti sulla macchina o alterare il sistema operativo o la configurazione dei programmi e dell'hardware della macchina .
- E' fatto obbligo di adottare comportamenti idonei a non provocare danni o pericoli agli strumenti ed alle attrezzature messi a disposizione . In caso di comodato d'uso dei device di proprietà o in concessione all'Istituto si fa riferimento al contratto.
- Gli utenti sono tenuti a non prelevare o depositare informazioni, applicazioni o documenti che possano in qualsiasi modo arrecare danno a persone , cose o all'Istituzione.
- E' vietato inserire file sul server o scaricare da internet software non autorizzati o materiale soggetto a copyright o a diritti di proprietà intellettuale.
- Il riscontro di qualsiasi anomalia deve essere tempestivamente segnalato dagli alunni al docente e dal docente al responsabile del laboratorio, al DS o a uno dei suoi collaboratori.
- Per utilizzare CD-ROM , DVD , penne USB o altri supporti di memorizzazione personali è necessario sottoporli al controllo anti virus.
- Si devono rispettare le regole di decenza e morali, evitare atti e comportamenti che possano recare offesa a cose , persone o istituzioni presenti o meno sulla rete.

- E' fatto assoluto divieto di navigare in siti dai contenuti pornografici o contenenti scene di violenza , razzismo o sfruttamento dei minori.
- Si deve mantenere segreto il nome, l'indirizzo, il telefono di casa, il telefono cellulare , il nome e l'indirizzo della scuola frequentata.
- Non si devono inviare a nessuno fotografie proprie o di amici.
- I docenti che accompagnano gli allievi in laboratorio o fanno usare i dispositivi di classe o i loro dispositivi (vedasi BYOD) sono tenuti a controllare che vengano rispettati i divieti sopraelencati che l'utilizzo delle risorse tecnologiche sia finalizzato agli intenti didattici previsti.

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 sarà affidato al referente del bullismo/cyberbullismo e al suo gruppo di lavoro. L'aggiornamento della e-policy sarà curato dal Dirigente scolastico, dal referente del bullismo/cyber bullismo, dal team digitale, sulla base delle segnalazioni effettuate dal personale della scuola.

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.
- Organizzare incontri per la consultazione degli studenti/studentesse sui temi dell'ePolicy per cui si evidenzia la necessità di regolamentare azioni e comportamenti.
 - Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i genitori dell'Istituto per la stesura finale dell'ePolicy.
 - Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto agli studenti
 - Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai docenti
 - Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai genitori
 - Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto agli studenti
 - Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai docenti
 - Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai genitori

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.
- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i genitori dell'Istituto per la stesura finale dell'ePolicy.
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto agli studenti
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai docenti
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai genitori
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto agli studenti
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai docenti
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai genitori

Capitolo 2 - Formazione e curriculum

2.1. Curriculum sulle competenze digitali per gli studenti

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

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

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

La scuola ha costruito il curriculum verticale delle competenze digitali facendo riferimento ai seguenti documenti:

- DigComp 2.1.: “Il quadro di riferimento per le competenze digitali dei cittadini”, con otto livelli di padronanza ed esempi di utilizzo.
 - [Raccomandazione del Consiglio europeo relativa alle competenze chiave per l’apprendimento permanente \(C189/9, p. 9\)](#).
 - Sillabo sull’educazione civica digitale del MIUR.
-

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 nostro Istituto, attraverso il collegio dei docenti, riconosce e favorisce la partecipazione del personale ad iniziative promosse sia direttamente dalla scuola (con il supporto 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.

La recente pandemia ha forzatamente implementato l'uso delle TIC come strumento fondamentale per la prosecuzione delle attività didattiche; ne è derivato un maggiore uso da parte dei docenti e di conseguenza da parte degli alunni. La maggiore attenzione all'uso delle tecnologie, in modo strutturato e integrato alla didattica tradizionale ha reso gli apprendimenti più motivanti, coinvolgenti ed inclusivi permettendo allo stesso docente di guidare i propri studenti nella fruizione dei contenuti online. Promuovere e implementare i corsi di formazione dei docenti è e sarà una priorità del nostro istituto.

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

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

territorio (USR, Osservatori regionali sul bullismo, scuole Polo, etc...), delle amministrazioni comunali, dei servizi socio-educativi e delle associazioni presenti.

Nell'ottica di creare ulteriore sinergia fra scuola, studenti/studentesse e famiglie, di promuovere la condivisione di buone pratiche nell'utilizzo consapevole delle TIC e di prevenire e contrastare ogni forma di discriminazione, offesa, denigrazione e lesione della dignità dell'altro, nonché fenomeni di bullismo e cyberbullismo, i docenti dell'Istituto scolastico facenti parte del team per il contrasto del bullismo/cyberbullismo hanno seguito i corsi sulla "Piattaforma Elisa" ; per gli altri insegnanti sarà previsto un percorso formativo specifico ed adeguato che abbia ad oggetto non solo l'uso responsabile e sicuro della Rete ma anche i rischi legati a quest'ultima.

Sono stati inoltre organizzati incontri con la Polizia di Stato per trattare le tematiche legate ai "Pericoli di internet".

L'Istituto organizzerà per gli insegnanti momenti di formazione e informazione che mettano al centro i temi in oggetto, considerando anche percorsi di autoaggiornamento personali o collettivi, iniziative seminariali con professionisti-esperti interni (si pensi al supporto dell'Animatore digitale e del Referente al Bullismo /Cyberbullismo) ed esterni alla scuola, giornate-settimane di approfondimento in accordo con la rete scolastica del territorio (USR, Osservatori regionali sul bullismo, scuole Polo, etc...),

con l'Amministrazione comunale, con i servizi socio-educativi e le associazioni/enti presenti sul territorio. Tali azioni programmatiche saranno inserite nel Piano triennale dell'offerta formativa.

Saranno previsti ulteriori incontri formativi/informativi con gli studenti, le famiglie e il personale scolastico per sensibilizzare tutta la comunità educante ad un corretto uso delle tecnologie e della rete.

Sarà predisposta un'area specifica sul sito dell'Istituto con materiali formativi e informativi per tutti gli operatori della scuola, per gli studenti e per le famiglie sull'utilizzo consapevole e sicuro di Internet.

Sempre sul sito istituzionale della scuola, sarà incluso il link e i materiali informativi del progetto "**Generazioni connesse**" (www.generazioniconnesse.it) dove trovare ulteriori approfondimenti, spunti aggiornamenti e strumenti didattici utili da usare con gli studenti e le studentesse, per ciascun grado di scuola.

2.4. - Sensibilizzazione delle famiglie e integrazioni al Patto di Corresponsabilità

Nella prevenzione dei rischi connessi ad un uso non consapevole delle TIC, così come nella promozione di un loro uso positivo e capace di coglierne le opportunità, è necessaria la collaborazione di tutti gli attori educanti, ognuno secondo i propri ruoli e le proprie responsabilità. Scuola e famiglia devono rinforzare l'alleanza educativa e promuovere percorsi educativi continuativi e condivisi per accompagnare insieme ragazzi/e e bambini/e verso un uso responsabile e arricchente delle tecnologie digitali, anche in una prospettiva lavorativa futura. L'Istituto garantisce la massima informazione alle famiglie di tutte le attività e iniziative intraprese sul tema delle tecnologie digitali, previste dall'ePolicy e dal suo piano di azioni, anche attraverso l'aggiornamento, oltre che del regolamento scolastico, anche del "Patto di corresponsabilità" e attraverso una sezione dedicata sul sito web dell'Istituto.

Anche alle famiglie verranno proposti incontri informativi e/o formativi sull'uso consapevole delle nuove tecnologie grazie ai quali verranno messi al corrente dei rischi nei quali i figli potrebbero imbattersi se non monitorati.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2019/2020)

Scegliere almeno 1 di queste azioni

- 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.
- Coinvolgere una rappresentanza dei genitori per individuare i temi di maggiore interesse nell'ambito dell'educazione alla cittadinanza digitale.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie

digitali.

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

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

Scegliere almeno 1 di queste azioni

- 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.
- Coinvolgere una rappresentanza dei genitori per individuare i temi di maggiore interesse nell'ambito dell'educazione alla cittadinanza digitale.
- 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.

I dati personali dello studente e dei loro familiari sono utilizzati dall'Istituto Comprensivo "S. Scandura" di Aci Catena, che ne è titolare per il trattamento, nel rispetto dei principi di protezione dei dati personali stabiliti dal Regolamento GDPR 2016/679, di seguito Regolamento, e del Decreto Legislativo n. 196/2003, di seguito come Codice. Il trattamento dei dati personali sarà improntato ai principi di liceità, correttezza e trasparenza ed effettuato attraverso l'adozione di misure tecniche ed organizzative opportunamente identificate al fine di garantire ai suoi dati riservatezza, correttezza ed integrità e diritti.

Il minore di età inferiore a 16 anni è rappresentato dai propri tutori legali che prestano il consenso quando previsto.

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.

Tutte le aule dell'Istituto sono fornite di copertura Wi-Fi.

Gli alunni hanno accesso alla Rete esclusivamente attraverso il PC posto in ogni aula.

I docenti possono accedere alla Rete per questioni meramente didattiche e sono dotati di una password personale permanente.

La Scuola, inoltre, garantisce l'accesso degli studenti alla Rete attraverso i PC dei laboratori informatici, ove presenti, e si è dotata di tutte le precauzioni necessarie per evitare l'accesso online a materiali non adatti all'età degli studenti e delle studentesse.

Gestione accessi (password, backup, ecc.)

L'accesso agli strumenti informatici è consentito al personale della scuola solo previa autenticazione effettuata mediante sistema di identificazione (attribuzione individuale di nome utente e password).

Ciascun utente è personalmente responsabile dell'uso del proprio account ed è tenuto a tutelarlo da accessi non autorizzati. Non è ammessa la comunicazione del proprio account a terzi.

La password è personale, riservata e non può essere ceduta o comunicata ad alcuno. È pertanto **vietato l'uso della password di altri utenti**; qualora se ne venisse a conoscenza è obbligatorio segnalare il fatto all'utente interessato, all'Animatore Digitale ed all'Amministratore di sistema.

È obbligatorio modificare la password ogni volta che il sistema ne faccia richiesta.

Per esigenze operative o di sicurezza e integrità del sistema e dei dati,

L'Amministratore di sistema ha facoltà di modificare la password degli utenti o di disabilitarle.

E-mail.

L'Istituto ha un account di posta elettronica istituzionale utilizzato esclusivamente dagli uffici amministrativi. La posta elettronica è protetta da sistemi antivirus, e quella certificata anche da sistemi antispam.

Con l'attivazione della piattaforma Gsuite (Google for education) tutti i Docenti e gli alunni hanno una e mail con il dominio della scuola.

Sito web della scuola

La scuola attualmente ha un sito web. Tutti i contenuti del settore didattico sono pubblicati direttamente e sotto supervisione del Dirigente scolastico che ne valuta la sicurezza e l'adeguatezza sotto i diversi profili dell'accessibilità, della pertinenza dei contenuti, del rispetto della privacy, ecc.

Social network.

La scuola ha attivato una pagina Facebook per consolidare l'identità della scuola e la sua visibilità nel contesto territoriale. Così come per il sito Web tutti i contenuti sono pubblicati da personale incaricato che con il Dirigente Scolastico ne valuta la sicurezza, l'adeguatezza sotto i diversi profili dell'accessibilità, della pertinenza dei contenuti, del rispetto della privacy, ecc.

La Pagina mira a trasmettere all'esterno i valori, le azioni, i progetti e l'idea di educazione che l'Istituto porta avanti.

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 che la scuola utilizza per raggiungere il personale, le famiglie e gli esterni è il sito web dell'Istituto, costantemente aggiornato con le notizie e i link d'interesse per l'utenza. Il sito web della scuola è pubblico e contiene documenti, informazioni e immagini non lesive della privacy degli utenti. La scuola detiene i diritti d'autore dei documenti che pubblica o dei documenti di cui ha ottenuto permesso dell'autore proprietario. Raccoglie, altresì, specifiche autorizzazioni del caso.

Per le comunicazioni generali al personale ed alle famiglie viene, altresì, utilizzata la sezione "bacheca" del Registro Elettronico ed attraverso le mail istituzionali con dominio @icscandura.edu.it. Invece, per quanto riguarda le comunicazioni relative ai singoli alunni o alle singole classi (ivi comprese quelle relative agli esiti degli esami o degli scrutini), si utilizza, in maniera esclusiva, la sezione "riservata" del registro elettronico. Durante la Didattica a Distanza (DaD) e la Didattica Digitale Integrata (DDI) la piattaforma utilizzata è Google GSuite. Questa permette la creazione di classi virtuali che consentono lo scambio reciproco di materiale fra docenti e studenti; l'accesso alla piattaforma avviene previo inserimento delle credenziali comunicate alle famiglie.

Gli indirizzi mail personali dei docenti e del personale scolastico non vengono pubblicati, né condivisi con gli alunni e le loro famiglie. Gli unici indirizzi da utilizzare in caso di comunicazione sono quelli presenti sul sito istituzionale. La comunicazione alle famiglie della mail personale o dei contatti telefonici privati è a discrezione di ogni docente e, ad ogni modo, non rappresenta un canale ufficiale di comunicazione.

In riferimento all'uso degli strumenti di comunicazione online per la circolazione di informazioni e comunicazione interne, come avviene generalmente fra i docenti mediante, ad esempio, l'uso di gruppi whatsapp o telegram, è importante ricordare che si tratta di canali utilizzati per velocizzare la trasmissione delle informazioni istituzionali che, successivamente, vengono formalizzate e rese ufficiali.

Relativamente al "diritto alla disconnessione", l'art. 22 (Livelli, soggetti, materie di relazioni sindacali per la Sezione Scuola) del CCNL 2016/2018, 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. Al proposito, è importante però ricordare che le chat informali fra colleghi o fra docenti e genitori, non rientrano nella fattispecie di cui all'art. 22 del CCNL; inoltre, relativamente al loro utilizzo, poiché non esistono regole di comportamento volte a favorire il reciproco rispetto tra gli utenti, è fondamentale partire dal buon senso, da una riflessione sulle peculiarità del mezzo e dalla definizione delle regole condivise sull'uso delle stesse. Fra queste, ad esempio, ve ne suggeriamo alcune:

- Mettere in chiaro fin dall'inizio, comprendere e rispettare sempre le finalità del gruppo, scrivendo e pubblicando solo contenuti pertinenti a tali finalità;
- Usare sempre un linguaggio adeguato e il più possibile chiaro e preciso (come già sottolineato la comunicazione online si presta spesso a non pochi

fraintendimenti);

- Evitare di affrontare in chat argomenti troppo complessi e controversi (la comunicazione online in una chat di gruppo non è adatta per la gestione di problematiche di questo tipo, che certamente è più opportuno affrontare in presenza o in un Consiglio di classe);
- 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 il più possibile 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.

3.4 - Strumentazione personale

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

La presente **ePolicy** contiene indicazioni, revisioni o eventuali integrazioni di Regolamenti già esistenti che disciplinano l'uso dei dispositivi personali in classe, a seconda dei vari usi, anche in considerazione dei dieci punti del Miur per l'uso dei dispositivi mobili a scuola (BYOD, "Bring your own device").

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

Come indicato nel Regolamento di disciplina:

- Per gli studenti: gestione degli strumenti personali - cellulari, tablet ecc.

Durante lo svolgimento delle attività didattiche è vietato l'uso dei cellulari e di altri dispositivi elettronici. L'uso del cellulare è consentito solo in caso di urgenza per comunicazioni tra gli alunni e le famiglie, su autorizzazione e con controllo dell'identità dell'interlocutore verificata

dal docente qualora non sia possibile utilizzare il telefono della scuola.

L'eventuale utilizzo di strumenti informatici di proprietà dello studente durante l'attività didattica deve essere autorizzato dal docente. A tal proposito sarà ovviamente consentito l'uso di dispositivi mobili personali durante le attività didattiche che ne prevedano l'utilizzo, secondo il regolamento BYOD (Bring your own device).

Particolare attenzione verrà riservata agli alunni con BES

- Per i docenti: gestione degli strumenti personali- cellulari, tablet ecc.

Durante le ore delle lezioni è consentito l'utilizzo del cellulare e di altri dispositivi elettronici personali, solo a scopo didattico ed integrativo rispetto a quelli disponibili. Durante il restante orario di servizio è consentito l'utilizzo dei dispositivi elettronici personali per attività funzionali all'insegnamento, ad integrazione di quelli messi a disposizione dalla scuola.

Per il personale della scuola: gestione degli strumenti personali - cellulari, tablet ecc.

Durante l'orario di servizio, a tutto il personale scolastico è consentito l'utilizzo del cellulare esclusivamente per comunicazioni di servizio e/o personali di carattere urgente.

Il nostro piano d'azioni

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

Scegliere almeno 1 di queste azioni:

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli studenti e delle studentesse
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte dei docenti
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte del personale Tecnico Amministrativo e dagli ATA
- Organizzare uno o più eventi o attività volti a consultare i docenti dell'Istituto per redigere o integrare

indicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola

- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare i genitori dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali

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

Scegliere almeno 1 di queste azioni:

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

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

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, come ha già fatto in passato, attiverà azioni di sensibilizzazione e prevenzione dei rischi online per ottenere i seguenti benefici i:

- accrescere la consapevolezza circa i rischi online negli alunni;
- incoraggiare i ragazzi a modificare i propri comportamenti rendendoli più

funzionali;

- diffondere all'esterno del gruppo di riferimento e quindi tra l'opinione pubblica una certa consapevolezza rispetto all'argomento di interesse;
 - facilitare il coinvolgimento di soggetti esterni in modo da mettere insieme diverse idee per lavorare ad un obiettivo comune.
 - favorire la diffusione di informazioni e servizi disponibili all'utilità collettiva (intervento di sensibilizzazione per promuovere la conoscenza dell'ePolicy nella comunità scolastica).
-

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).

Una parte del personale ha partecipato a corsi di formazione sul cyberbullismo sulla piattaforma Elisa; la scuola, attraverso il referente e i docenti ha sensibilizzato e sensibilizzerà ancora gli alunni in merito a questa tematica, seguendo le indicazioni date ed il materiale reperibile in piattaforma. Anche i corsi della piattaforma "Generazioni connesse" hanno dato indicazioni, materiali e un percorso con video interattivi per affrontare la tematica in modo coinvolgente e partecipato.

Le azioni di prevenzione hanno inoltre visto e vedranno ancora l'intervento della Polizia di Stato del distretto di Acireale. La presenza di un referente e di un team all'interno della scuola sottolinea la volontà dell'istituzione di prevenire e contrastare il fenomeno.

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.

L'Istituto, pur non dedicando attività specifiche alla prevenzione dell'hate speech, favorisce in ogni momento la costruzione di una modalità d'intervento non ostile e non basata su stereotipi offensivi.

Ogni docente, all'interno delle sue discipline e delle sue ore con gli studenti e le studentesse, dedica tempo ed energie alla costruzione di un ascolto attivo e di un dialogo pacifico. Attraverso le attività che vengono proposte dai docenti, gli studenti e le studentesse vengono aiutati a riflettere sul concetto d'identità, propria ed altrui e a decostruire quegli stereotipi su cui spesso si fonda l'hate speech.

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 dipendenza da Internet, che può manifestarsi anche attraverso le ore trascorse online a giocare, rappresenta una questione importante per la comunità scolastica che deve attenzionare il fenomeno e fornire gli strumenti agli studenti e alle studentesse affinché questi siano consapevoli dei rischi che comporta l'iperconnessione.

Spesso il trascorrere del tempo online, in termini disfunzionali, è scandito dal gioco virtuale che può anche assumere forme di Dipendenza dal gioco online inserito all'interno del Manuale Diagnostico Statistico dei Disturbi Mentali (DSM 5). Da specificare che la dipendenza qui si realizza quando c'è un abuso, ossia un utilizzo continuativo e sistematico della Rete al fine di giocare impegnando la maggior parte delle giornate, con la conseguente sottrazione del tempo alle altre attività quotidiane del minore.

Di seguito i sintomi che devono essere presenti (per un arco di tempo di almeno un anno):

1. il giocatore è assorbito totalmente dal gioco;
2. il giocatore è preoccupato e ossessionato dal gioco (si veda Lancini M., Il ritiro sociale negli adolescenti, Raffaello Cortina Ed.,

Milano, 2019);

3. il gioco consente alla persona di sfuggire alla realtà con la sperimentazione di emozioni più piacevoli;
4. il giocatore manifesta sempre di più l'impulso di giocare e di sperimentare emozioni positive;
5. il giocatore sente di dover dedicare più tempo ai giochi;
6. il giocatore se non può giocare manifesta ansia, depressione e irritabilità;
7. può emergere un ritiro sociale (si veda il punto 3);
8. il giocatore, anche se comprende la gravità della situazione e sospende di giocare comunque non riesce a interrompere del tutto;
9. il giocatore mente agli altri sull'utilizzo che fa dei giochi on line;
10. il giocatore ha perso o mette a rischio relazioni o opportunità a causa dei giochi su Internet o ha perso interesse verso attività nella vita reale.

Anche in questo caso, la scuola ha la possibilità di fare formazione e di indicare strategie 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.

La tecnologia infatti ha modificato gli ambienti che viviamo e ha un impatto sulla qualità della vita. Gli [elementi che contribuiscono al benessere digitale sono:](#)

- 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)

La scuola durante le lezioni di cittadinanza digitale dedicherà al tema un momento specifico per riflettere con studenti e studentesse e fare in modo che la tecnologia sia strumento per raggiungere i propri obiettivi

e non sia solo distrazione o addirittura ostacolo.

Si cercherà di integrare la tecnologia nella didattica, mostrando un suo utilizzo funzionale che possa rendere più consapevoli i ragazzi e le ragazze delle proprie abitudini online.

Gli insegnanti faranno riflettere gli alunni ponendo loro queste domande: come trascorri il tempo on line? Quando aggiunge valore alla tua vita e quando ti fa perdere tempo? Quale atteggiamento potrei cambiare quando sono online? Che ruolo ha e deve avere la tecnologia (internet o il gioco) nella mia vita?

Allo stesso modo quando si parlerà di videogiochi, gli insegnanti cercheranno di pensarli non in termini negativi ma di benessere digitale. Sono parte del mondo di studenti e studentesse. E, allora: quando sono una risorsa? Accedono a contenuti adeguati all'età? A che ora e per quanto tempo li usano?

Diventerà utile riflettere con i ragazzi e le ragazze rispetto all'uso della tecnologia in termini di qualità e tempo.

La scuola si impegnerà a non demonizzare la tecnologia o il gioco ma a **strutturare regole condivise** e stipulare con i ragazzi una sorta di "patto" d'aula e, infine, proporre delle alternative metodologiche e didattiche valide che abbiano come strumento giochi virtuali d'aula (Es. adoperando la LIM o il dispositivo personale. Si veda il BYOD di cui abbiamo parlato nel precedente modulo.

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 medialmente 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 proporrà la realizzazione di percorsi di sensibilizzazione e prevenzione dedicati a:

- Educazione all'affettività e alla sessualità (anche online)
- Immagine di sé online
- Relazioni online

La scuola inoltre pubblicherà sul sito web una guida operativa rivolta a genitori, insegnanti e operatori della scuola (Vademecum di "Generazioni Connesse") con l'obiettivo di diffondere, soprattutto a livello territoriale, strumenti conoscitivi ed operativi utili per orientarsi nella gestione di alcune problematiche inerenti l'utilizzo delle Tecnologie dell'Informazione e della Comunicazione (TIC) da parte dei più giovani.

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.

La scuola sensibilizzerà gli alunni sulla tematica e pubblicherà sul sito web una guida operativa rivolta a genitori, insegnanti e operatori della scuola (Vademecum di "Generazioni Connesse") con l'obiettivo di diffondere, soprattutto a livello territoriale, strumenti conoscitivi ed operativi utili per orientarsi nella gestione di alcune problematiche inerenti l'utilizzo delle Tecnologie dell'Informazione e della Comunicazione (TIC) da parte dei più giovani.

4.7 - Pedopornografia

La pedopornografia online è un reato (art. 600-ter comma 3 del c.p.) che consiste nel produrre, divulgare, diffondere e pubblicizzare, anche per via telematica, immagini o video ritraenti bambini/e, ragazzi/e coinvolti/e in comportamenti sessualmente espliciti, **concrete o simulate** o qualsiasi rappresentazione degli organi sessuali a fini soprattutto sessuali.

La legge n. 269 del 3 agosto 1998 *“Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di schiavitù”*, introduce nuove fattispecie di reato (come ad esempio il turismo sessuale) e, insieme alle successive modifiche e integrazioni contenute nella **legge n. 38 del 6 febbraio 2006** *“Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet”*, segna una tappa fondamentale nella definizione e predisposizione di strumenti utili a contrastare i fenomeni di sfruttamento sessuale a danno di minori. Quest’ultima, introduce, tra le altre cose, il reato di “pornografia minorile virtuale” (artt. 600 ter e 600 quater c.p.) che si verifica quando il materiale pedopornografico rappresenta immagini relative a bambini/e ed adolescenti, realizzate con tecniche di elaborazione grafica non associate, in tutto o in parte, a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali.

Secondo la Legge 172/2012 - Ratifica della Convenzione di Lanzarote (Art 4.) per pornografia minorile si intende ogni rappresentazione, con qualunque mezzo, di un minore degli anni diciotto coinvolto in attività sessuali esplicite, reali o simulate, o qualunque rappresentazione degli organi sessuali di un minore di anni diciotto per scopi sessuali.

In un’ottica di attività preventive, il tema della pedopornografia è estremamente delicato, occorre parlarne sempre in considerazione della maturità, della fascia d’età e selezionando il tipo di informazioni che si possono condividere.

La pedopornografia è tuttavia un fenomeno di cui si deve sapere di più, ed è utile parlarne, in particolare se si vogliono chiarire alcuni aspetti legati alle conseguenze impreviste del sexting.

Inoltre, è auspicabile che possa rientrare nei temi di un’attività di sensibilizzazione rivolta ai genitori e al personale scolastico promuovendo i servizi di Generazioni Connesse: qualora navigando in Rete si incontri materiale pedopornografico è opportuno segnalarlo, anche anonimamente, attraverso il sito www.generazioniconnesse.it alla sezione **“Segnala contenuti illegali” (Hotline)**.

Il servizio Hotline si occupa di raccogliere e dare corso a segnalazioni, inoltrate anche in forma anonima, relative a contenuti pedopornografici e altri contenuti illegali/dannosi diffusi attraverso la Rete. I due servizi messi a disposizione dal Safer Internet Centre sono il “Clicca e Segnala” di [Telefono Azzurro](#) e “STOP-IT” di [Save the Children](#).

La scuola sensibilizzerà gli alunni sulla tematica e pubblicherà sul sito web una guida operativa rivolta a genitori, insegnanti e operatori della scuola (Vademecum di "Generazioni Connesse") con l'obiettivo di diffondere, soprattutto a livello territoriale, strumenti conoscitivi ed operativi utili per orientarsi nella gestione di alcune problematiche inerenti l'utilizzo delle Tecnologie dell'Informazione e della Comunicazione (TIC) da parte dei più giovani.

Il nostro piano d'azioni

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

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 agli/le studenti/studentesse, con il coinvolgimento di esperti.
- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti.
- Promuovere incontri e laboratori per studenti e studentesse dedicati all'Educazione Civica Digitale.
- Organizzare uno o più incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/le studenti/studentesse.
- Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/le studenti/studentesse.
- Pianificare e realizzare progetti di peer-education - sui temi della sicurezza online - nella scuola.

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 agli/le studenti/studentesse, con il coinvolgimento di esperti.
- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti.
- Promuovere incontri e laboratori per studenti e studentesse dedicati all'Educazione Civica Digitale.
- Organizzare uno o più incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/le studenti/studentesse.
- Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/le studenti/studentesse.
- 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 minorenni e inoltre è importante non sostituirsi al bambino/a e/o adolescente, evitando, quindi, di rispondere all'adescatore al suo posto). È fondamentale valutare il benessere psicofisico dei minori e il rischio che corrono. Vi ricordiamo che l'attuale normativa prevede che la persona coinvolta in qualità di vittima o testimone in alcune tipologie di reati, tra cui il grooming, debba essere ascoltata in sede di raccolta di informazioni con l'ausilio di una persona esperta in psicologia o psichiatria infantile.
- **Sexting:** nel caso in cui immagini e/o video, anche prodotte autonomamente da persone minorenni, sfuggano al loro controllo e vengano diffuse senza il loro consenso è opportuno adottare sistemi di segnalazione con l'obiettivo primario di tutelare il minore e ottenere la rimozione del materiale, per quanto possibile, se online e il blocco della sua diffusione via dispositivi mobili.

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

Vi suggeriamo, inoltre, i seguenti servizi:

- Servizio di [Helpline 19696](#) e [Chat di Telefono Azzurro](#) per supporto ed emergenze;
- [Clicca e segnala di Telefono Azzurro](#) e [STOP-IT di Save the Children Italia](#) per

segnalare la presenza di materiale pedopornografico online.

5.2. - Come segnalare: quali strumenti e a chi

L'insegnante riveste la qualifica di pubblico ufficiale in quanto l'esercizio delle sue funzioni non è circoscritto all'ambito dell'apprendimento, ossia alla sola preparazione e tenuta delle lezioni, alla verifica/valutazione dei contenuti appresi dagli studenti e dalle studentesse, ma si estende a tutte le altre attività educative.

Le situazioni problematiche in relazione all'uso delle tecnologie digitali dovrebbero essere sempre gestite anche a livello di gruppo.

Come descritto nelle procedure di questa sezione, si potrebbero palesare due casi:

- CASO A (SOSPETTO) - Il docente ha il sospetto che stia avvenendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.
- CASO B (EVIDENZA) - Il docente ha evidenza certa che stia accadendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.

Per tutti i dettagli fate riferimento agli allegati con le procedure.

Strumenti a disposizione di studenti/esse

Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione:

- un indirizzo e-mail specifico per le segnalazioni;
- scatola/box per la raccolta di segnalazioni anonime da inserire in uno spazio accessibile e ben visibile della scuola;
- sportello di ascolto con professionisti;

- docente referente per le segnalazioni.

Anche studenti e studentesse, inoltre, possono rivolgersi alla Helpline del progetto Generazioni Connesse, al numero gratuito [1.96.96](tel:1.96.96).

5.3. - Gli attori sul territorio

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

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

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

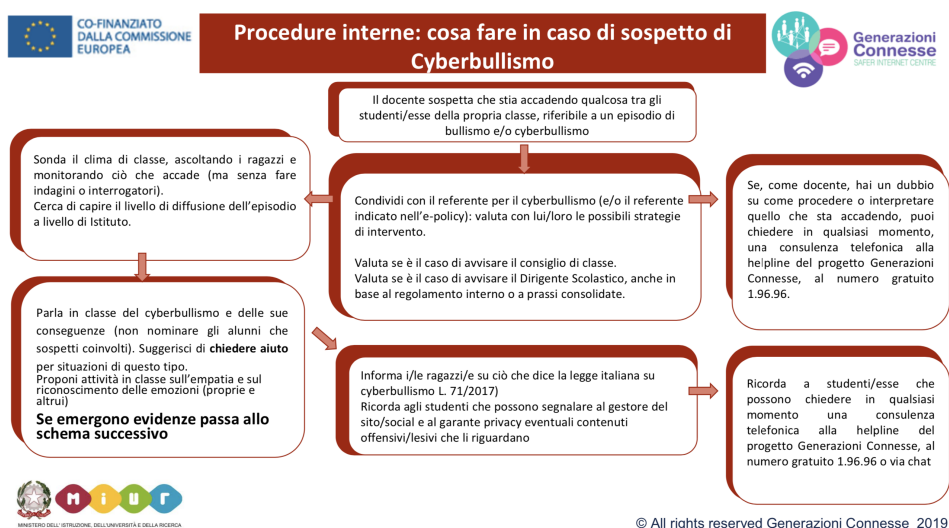
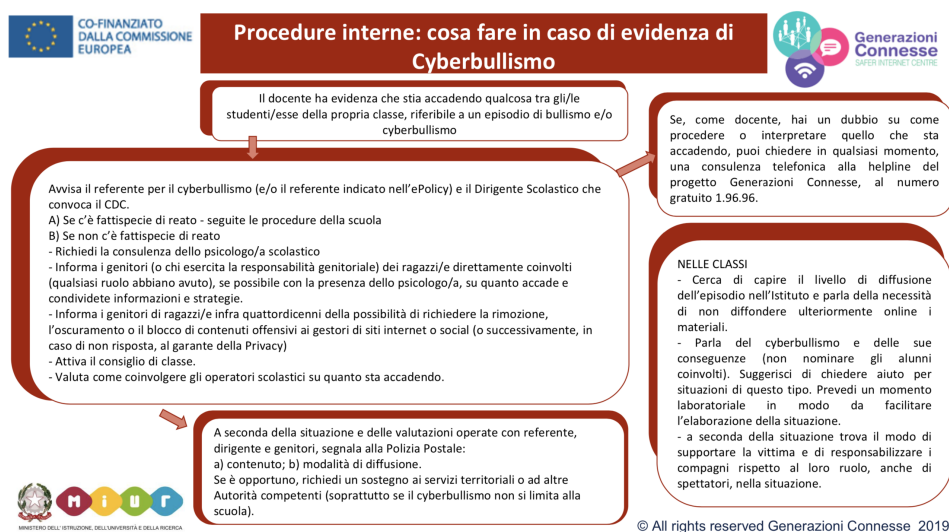
- **Comitato Regionale Unicef:** laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell’infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni):** svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare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

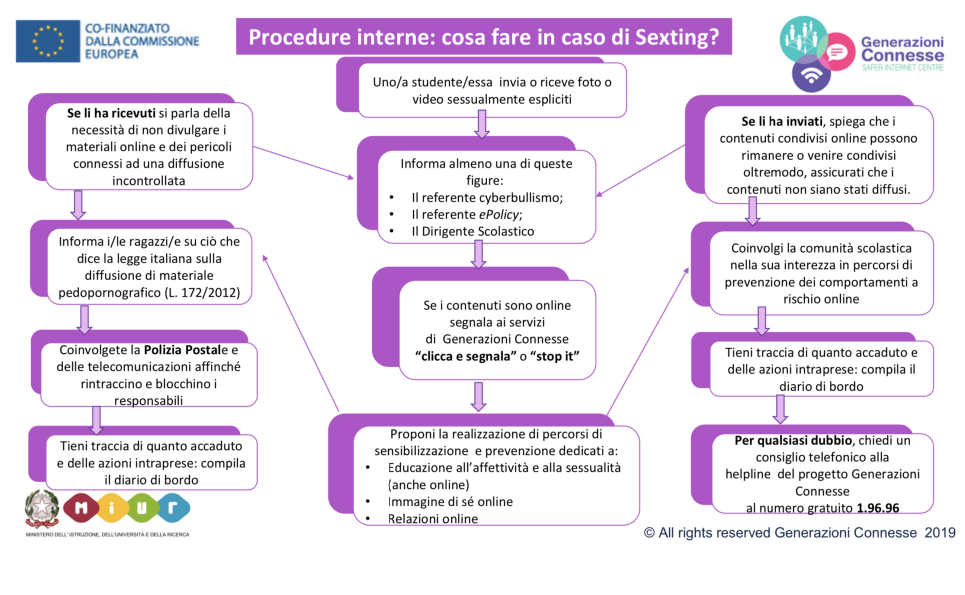
- **Tribunale per i Minorenni:** segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

5.4. - Allegati con le procedure

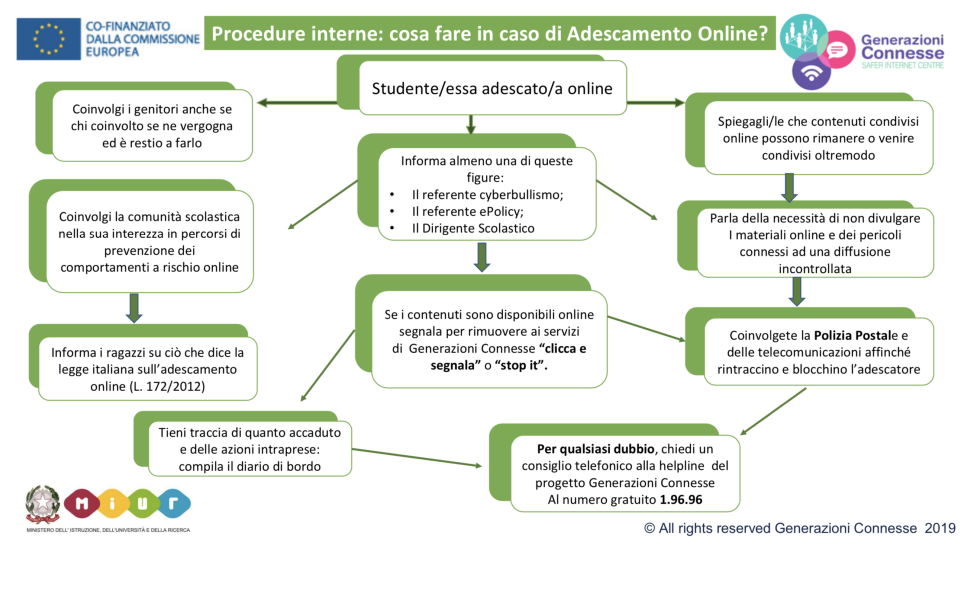
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



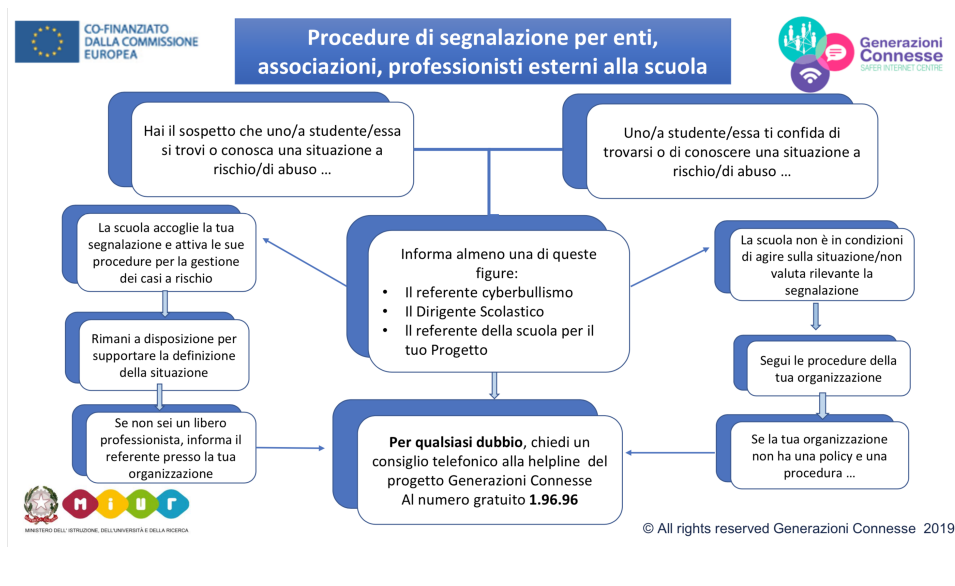
Procedure interne: cosa fare in caso di sexting?



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.

