



I.I.S.S. "M. GIUA" CAGLIARI
Prot. 0009774 del 26/05/2023
IV (Entrata)



Istituto di Istruzione Superiore
Michele Giua Cagliari

Documento di ePolicy

CATF04000P

I.T.I. "M. GIUA" CAGLIARI

VIA MONTECASSINO - 09134 - CAGLIARI - CAGLIARI (CA)

Maria Romina LAI

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.

La diffusione dei social fra gli adolescenti ha influenzato le modalità di accesso all'informazione e ha ridefinito le dinamiche comunicativo-relazionali. Tuttavia, se la Rete rappresenta per i più giovani una indubbia fonte di opportunità e stimoli di natura cognitiva, comunicativa e relazionale, d'altro canto un utilizzo scorretto potrebbe esporre a situazioni di vulnerabilità.

In una simile situazione la Scuola, luogo di formazione, inclusione e accoglienza, ha il dovere di mediare il rapporto tra gli adolescenti e le nuove tecnologie digitali, promuovendone un uso sicuro, consapevole ed efficace.

Il Ministero dell'istruzione è impegnato da anni sul fronte della prevenzione del fenomeno del bullismo e del cyberbullismo e più in generale, di ogni forma di violenza. Diverse sono le strategie di intervento utili ad arginare i comportamenti a rischio, attraverso il [Decreto prot. n. 1176 del 18/05/2022 - Assegnazione fondi per contrastare il fenomeno del cyberbullismo \(Legge n.234/2021\)](#)

Decreto assegnazione fondi per contrastare il fenomeno del cyberbullismo da destinare agli Uffici Scolastici Regionali, la Legge 107 del 2015 ha introdotto, tra gli obiettivi formativi prioritari, lo sviluppo di competenze digitali negli studenti per un uso critico e consapevole dei social network e dei media. La Legge 71 del 2017 ha sancito un ulteriore obiettivo strategico: contrastare il fenomeno del cyberbullismo in tutte le sue manifestazioni. Azioni a carattere preventivo e strategie di attenzione, tutela ed educazione entrano in campo nei confronti dei minori coinvolti, sia in quanto vittime sia come responsabili di illeciti, per assicurare l'attuazione degli interventi senza distinzione di età nell'ambito delle istituzioni scolastiche. L'aggiornamento 2021 delle Linee Guida per la prevenzione e il contrasto del Bullismo e Cyberbullismo (Decreto ministeriale 18 del 13 gennaio 2021 emanato con nota 482 del 18 febbraio 2021) consente a dirigenti, docenti e operatori scolastici di comprendere, ridurre e contrastare i fenomeni negativi che colpiscono bambine e bambini, ragazze e ragazzi, con nuovi strumenti.

Tali iniziative hanno trovato il loro coronamento nel progetto Generazioni Connesse, iniziativa sostenuta dalla Commissione Europea e coordinata dal MIUR, realizzata in partenariato con le principali Agenzie nazionali sensibili al tema della sicurezza in Rete. Il nostro Istituto, da sempre convinto dell'opportunità di integrare le nuove tecnologie nella didattica e sensibile al benessere psico-fisico dei propri studenti, si impegna quotidianamente nella promozione di valori e competenze finalizzate all'acquisizione di una cittadinanza digitale consapevole. Attraverso mirati interventi formativi, informativi e partecipativi, in sinergia con Enti territoriali e Agenzie

nazionali, l'Istituto intende orientare studentesse e studenti ad un uso responsabile della Rete, fornendo loro le giuste chiavi di lettura per la corretta gestione di relazioni digitali in luoghi e situazioni oggettivamente non protetti. In particolare, l'adesione al progetto Generazioni Connesse risponde proprio all'esigenza di sostenere studenti, ma anche famiglie e operatori scolastici sui temi della e-Safety mediante nuovi e più efficaci strumenti di contrasto.

Rientra in questa prospettiva la redazione della E-Policy, documento programmatico finalizzato a promuovere una coscienza digitale in quanti, da diverse angolature, sono coinvolti nel processo educativo.

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.

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. L'IIS "Michele Giua, al fine di rispondere efficacemente a tale esigenza, individua le seguenti figure, declinando per ciascuna gli specifici ambiti di intervento:

Il Dirigente Scolastico

il Dirigente Scolastico garantisce la sicurezza, anche online, di tutti i membri della comunità scolastica. E' importante, quindi, la sua adeguata formazione sulla sicurezza e sulla prevenzione di problematiche offline e online, in linea con il quadro normativo di riferimento e le indicazioni del MIUR; inoltre, promuove la cultura della sicurezza online e, ove possibile, dà il proprio contributo all'organizzazione, insieme al docente referente sulle tematiche del bullismo/cyberbullismo, di corsi di formazione specifici per tutte le figure scolastiche sull'utilizzo positivo e responsabile delle TIC. Vi ricordiamo, inoltre, che il Dirigente Scolastico ha la responsabilità di gestire ed intervenire nei casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali.

L'Animatore Digitale

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 gestione dei dati personali, oltre che essere uno dei promotori di percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale" (con riferimento, ad esempio,

allo sviluppo delle competenze digitali previste anche nell'ambito dell'educazione civica); potrebbe, inoltre, 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).

Il Referente bullismo e cyberbullismo

“Ogni Istituto scolastico, nell'ambito della propria autonomia, individua fra i docenti un referente con il compito di coordinare le iniziative di prevenzione e di contrasto del cyberbullismo” (Art. 4 Legge n.71/2017, “Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo” (permalink - file 1 LEGGE 71_2017 in allegato). Tale figura 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) potrebbe coinvolgere, con progetti e percorsi formativi ad hoc, studenti, colleghi e genitori (un approfondimento maggiore sui ruoli relativi alle problematiche del bullismo e del cyberbullismo verrà fornito nel modulo 4, al paragrafo 4.2.).

I Docenti

i Docenti hanno un ruolo centrale nel diffondere la cultura dell'uso responsabile delle TIC e della Rete. Potrebbero, innanzitutto, integrare parti del curriculum della propria disciplina con approfondimenti ad hoc, promuovendo, laddove possibile, anche l'uso delle tecnologie digitali nella didattica. I docenti dovrebbero 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; hanno il dovere morale e professionale di segnalare al Dirigente Scolastico qualunque problematica, violazione o abuso, anche online, che vede coinvolti studenti e studentesse.

Il personale Amministrativo, Tecnico e Ausiliario (ATA)

Il personale Amministrativo, Tecnico e Ausiliario (ATA) svolge funzioni miste, ossia di tipo amministrativo, contabile, gestionale e di sorveglianza connesse all'attività delle istituzioni scolastiche, in collaborazione con il dirigente scolastico e con il personale docente tutto. Diverse figure che, in sinergia, si occupano ciascuno per la propria funzione, del funzionamento dell'Istituto scolastico che passa anche attraverso lo sviluppo della cultura digitale e dell'organizzazione del tempo scuola. Esiste, cioè, 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 dovrebbe, all'interno dei singoli regolamenti d'Istituto, essere coinvolto nella segnalazione di 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

gli Studenti e le Studentesse dovrebbero, 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 dovrebbero imparare a tutelarsi online, tutelare i/le propri/e compagni/e e rispettarli/le; dovrebbero 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

i Genitori, in continuità con l'Istituto scolastico, dovrebbero 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; dovrebbero 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. È estremamente importante che accettino e condividano quanto scritto nell'ePolicy dell'Istituto.

Gli Enti educativi esterni e le associazioni

gli Enti educativi esterni e le associazioni che entrano in relazione con la scuola dovrebbero conformarsi alla politica della stessa riguardo all'uso consapevole della Rete e delle TIC; dovrebbero, inoltre, promuovere comportamenti sicuri, la sicurezza online e assicurare la protezione degli studenti e delle studentesse durante le attività che si svolgono insieme. A tal fine suggeriamo di prevedere una sezione specifica dell'ePolicy con indicazioni ad hoc e procedure standard per gli attori esterni.

Per un approfondimento sui ruoli e le responsabilità delle figure presenti a scuola: Legge 59/97, Art. 21 CO° 8; Legge N.165/2001 Art. 25; CCNL; DPR n. 275/99; Legge n.107/2015; Piano Nazionale Scuola Digitale.

Vi ricordiamo, inoltre, 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.

1.3 - Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto

Tutti gli attori che entrano in relazione educativa con gli studenti e le studentesse devono: mantenere sempre un elevato profilo personale e professionale, eliminando atteggiamenti inappropriati, essere guidati dal principio di interesse superiore del minore, ascoltare e prendere in seria considerazione le opinioni ed i desideri dei minori, soprattutto se preoccupati o allertati per qualcosa.

Sono vietati i comportamenti irrispettosi, offensivi o lesivi della privacy, dell'intimità e degli spazi personali degli studenti e delle studentesse oltre che quelli legati a tollerare o partecipare a comportamenti di minori che sono illegali, o abusivi o che mettano a rischio la loro sicurezza.

Tutti gli attori esterni sono tenuti a conoscere e rispettare le regole del nostro Istituto dove sono esplicitate le modalità di utilizzo dei propri dispositivi personali (smartphone, tablet, pc, etc.) e quelli in dotazione della scuola, evitando un uso improprio o comunque deontologicamente scorretto durante le attività con gli studenti e le studentesse. Esiste l'obbligo di rispettare la privacy, soprattutto dei soggetti minorenni, in termini di fotografie, immagini, video o scambio di contatti personali (numero, mail, chat, profili di social network).

da compilare con le indicazioni contenute nella lezione

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

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

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

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

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

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

Attraverso una serie di iniziative dedicate, l'IIS "Giua" si impegna ad assicurare la concreta promozione degli intenti dichiarati nel documento, valorizzando studenti e studentesse ed esplicitando ruoli e prerogative di tutte le figure operanti a vario titolo nella comunità scolastica. Il documento di E-policy sarà condiviso con tutta la comunità educante, ponendo al centro gli studenti e le studentesse e sottolineando compiti, funzioni e attività reciproche. L'E-policy sarà 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, sottoscritto dalle famiglie e rilasciato alle stesse all'inizio dell'anno scolastico. Il documento sarà approvato dal Collegio dei Docenti e dal Consiglio di Istituto. Al fine di comunicare al meglio il documento di ePolicy a tutta la comunità scolastica, sono previste le seguenti azioni: presentazione del documento ai docenti, al personale A.T.A., ai rappresentanti dei genitori e ai rappresentanti degli studenti durante specifici incontri, appositamente organizzati ad inizio anno scolastico, a tutte le classi, ad inizio anno scolastico, inserendo l'argomento nella programmazione didattica, all'interno dell'educazione alla cittadinanza digitale.

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.

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. In relazione all'uso improprio delle TIC a scuola da parte degli studenti e delle studentesse, sono sanzionate le seguenti condotte con gli strumenti disciplinari previsti dal Regolamento e decisi dal Consiglio di Classe: episodi di cyberbullismo; realizzazione e condivisione online, o anche solo condivisione, di immagini o video di compagni/e senza il loro consenso o che li ritraggono in pose offensive e denigratorie o comunque volti all'esclusione di compagni/e; realizzazione e condivisione, o anche solo condivisione, di scatti intimi e a sfondo sessuale; condivisione di dati personali di terzi (compagni, docenti, personale A.T.A.) senza il loro consenso; uso della rete per giudicare, infastidire o impedire a qualcuno di esprimersi o partecipare; condivisione in rete di comunicazione ufficiali interne all'Istituto: compiti in classe, circolari, comunicazioni, valutazioni e similari; registrazioni audio delle lezioni senza una preventiva autorizzazione da parte del docente; connessioni a siti proibiti o comunque non autorizzati; pirateria informatica; scaricamento di file (video, film, musica, immagini, test, ecc.) per finalità personali.

In relazione all'uso improprio delle TIC a scuola in situazioni in cui gli studenti risultino "vittime", sono segnalate agli organi territoriali competenti le seguenti condotte: possibile dipendenza (patologica) dalla rete (social network, gambling, vamping, esposizione a filmati violenti o a contenuto pedopornografico; relazioni pericolose/adescamento in rete; incitamento all'odio; divulgazione di notizie false.

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 Regolamento dell'Istituto Scolastico sarà 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 di ePolicy si integrerà pienamente con gli obiettivi enunciati nel PTOF, con il Regolamento di Istituto, con il Patto educativo di corresponsabilità controfirmato da Scuola, genitori e studenti all'atto dell'iscrizione e ci saranno opportuni riferimenti anche all'interno di tali documenti.

1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

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

L'ePolicy sarà riesaminata periodicamente e quando si verificano cambiamenti significativi in riferimento all'uso delle tecnologie digitali all'interno della scuola. L'Istituto si impegnerà a valutarne l'incidenza e l'efficacia con cadenza annuale e, prescindendo da tale tempistica, non solo ogni qual volta si dovessero verificare rilevanti variazioni in merito alla dotazione digitale della Scuola, ma anche qualora si rendessero necessari adeguamenti alla normativa sul tema. Ne verrà testata l'efficacia con particolare riferimento agli obiettivi in esso esplicitati: promozione delle competenze digitali e dell'uso delle TIC nei percorsi educativi e didattici, prevenzione e gestione dei rischi connessi alla Rete, tutela del benessere socio-relazionale delle studentesse e degli studenti.

Le modifiche del documento saranno discusse con tutti i membri del personale docente. Il monitoraggio del documento dovrebbe prevedere anche una valutazione della sua efficacia a partire dagli obiettivi specifici che lo stesso si pone. Il

monitoraggio e l'eventuale aggiornamento del documento è a cura del Dirigente scolastico, coadiuvato dall'Animatore digitale e dal Referente per il bullismo e il cyberbullismo, previa raccolta di feedback provenienti dalla comunità educante tutta.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

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

In ottemperanza alla L. 71/2017 -Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo-, il nostro Istituto realizza progetti volti all'educazione alla legalità e alla prevenzione delle nuove e pericolose forme di prevaricazione che hanno per teatro la Rete. In particolare, per tutte le classi prime e seconde viene annualmente programmato un incontro con la Polizia Postale finalizzato a sensibilizzare gli studenti rispetto all'uso consapevole di Internet e dei Social Network, educare al rispetto delle leggi che regolano il mondo virtuale, informare e responsabilizzare sul fenomeno del Cyberbullismo. Aderisce inoltre alle iniziative del Safer Internet Day, giornata mondiale per la sicurezza in Rete, istituita e promossa dalla Commissione europea. Da anni gli studenti partecipano a: #io non cado nella rete, torneo nazionale a squadre che incuriosisce e coinvolge i ragazzi sulla conoscenza e sulle problematiche che possono derivare da un uso poco consapevole della Rete. Il progetto è realizzato in collaborazione con il Dipartimento di Scienze Umane, Sociali e della Salute (L.A.P.A.SS.) dell'Università di Cassino e del

Lazio meridionale. Sono stati organizzati degli incontri online con l'associazione Bulli No Stop, nei quali i ragazzi sono stati messi a confronto con vittime del bullismo. Sono stati organizzati degli incontri a cadenza mensile con la onlus "Agape" che ha messo a confronto psicologi ed educatori con studenti e formatori. All'interno del progetto "Competenzecontrobullismo" sono stati somministrati dei questionari agli studenti per rilevare la percezione di queste problematiche all'interno delle classi. Da quest'anno l'Istituto partecipa inoltre al monitoraggio dei fenomeni di bullismo e cyberbullismo nelle scuole Italiane - Piattaforma ELISA.

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 PNSD promuove e valorizza il buon uso delle TIC nella didattica, estendendo il concetto di scuola da luogo fisico a spazio di apprendimento virtuale. In risposta alle sollecitazioni di un contesto socio- culturale in costante evoluzione, la Scuola ormai da tempo ha avviato una fase di ripensamento delle proprie strutture e dei propri assetti didattici in un'ottica digitale. L'introduzione delle Digital boards nelle classi rappresenta l'acme di questo processo. Considerevoli i vantaggi: l'impiego strutturato ed integrato delle TIC nella didattica, promuovendo un uso sincretico di più canali comunicativi, rende gli apprendimenti motivanti, coinvolgenti ed inclusivi, diversifica la prassi educativa, la rende innovativa e capace di offrire efficaci risposte ai diversi stili di apprendimento; non ultimo, stimola negli studenti la maturazione di senso critico rispetto all'eventuale fruizione di contenuti online. Ma affinché le potenzialità insite nell'uso delle TIC si trasformino in soluzioni concrete ed efficaci, è necessario che le vengano utilizzate in modo opportuno e significativo, con un adeguamento delle competenze degli insegnanti. Sono stati attivati dei corsi di formazione per il personale docente sull'utilizzo di nuova strumentazione digitale (ad es. VR per l'utilizzo nella didattica di strumentazione per realtà virtuale e aumentata).

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.

Al fine di favorire la condivisione di buone pratiche in materia di utilizzo consapevole e sicuro dei nuovi media, e prevenire e contrastare qualsivoglia forma di devianza e prevaricazione che abbia come scenario la rete, è, dunque, opportuno che i docenti seguano un percorso formativo dedicato. Agli aspetti di natura prettamente tecnica, connessi all'alfabetizzazione al digitale, si associano, in tal modo, riflessioni di carattere etico-morale; sarebbe infatti opportuno che disponessero di adeguati strumenti per educare i ragazzi alla gestione delle emozioni, per guidarli a discernere criticamente i pro dai contro e sensibilizzarli rispetto agli eventuali pericoli derivanti da un incauto approccio alla rete. Interessanti spunti di riflessione per i docenti e rimandi ad utili strumenti didattici sono presenti anche sul sito istituzionale della Scuola, dove è stato incluso il link relativo al progetto MIUR Generazioni connesse.

La nostra scuola intende promuovere specifici momenti di formazione permanente sul tema, in presenza o a distanza, incentivando percorsi di aggiornamento individuale o collettivo, iniziative seminariali in collaborazione con esperti interni - dall'Animatore digitale al Referente per il bullismo e il cyberbullismo - ed esterni.

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.

Solo mediante una attività divulgativa periodica sarà possibile rendere partecipi le famiglie dell'indirizzo che il nostro Istituto persegue in merito, delle strategie adottate per prevenire eventuali devianze, delle misure previste per contrastarle e degli eventuali provvedimenti sanzionatori da irrogare, commisurati all'entità del danno arrecato e sempre in un'ottica educativa e mai punitiva. Il Regolamento d'Istituto, cui è garantita massima diffusione mediante pubblicazione sul sito web della Scuola, è stato integrato con Il PROTOCOLLO DI INTERVENTO BULLISMO E CYBERBULLISMO, il documento è stato prodotto dal team contro il bullismo e il cyberbullismo, al fine di accrescere le conoscenze e le competenze degli operatori della scuola e delle famiglie, per accertare situazioni a rischio e individuare modalità che permettano di prevenire, affrontare e contrastare il fenomeno del cyberbullismo.

Il nostro piano d'azioni

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

- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare incontri con esperti per i docenti sulle competenze digitali

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.
- 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.

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.

La Scuola ha il dovere di considerare l'ambiente online alla stregua dell'ambiente fisico e valutarne tutti gli aspetti legati alla sicurezza, sia in termini di safety/prevenzione dei rischi, nonché di security, intesa come concreta risposta ai pericoli che rimandano alla sfera dell'illegalità. Da qui la necessità di tutelare la privacy degli studenti e delle loro famiglie, nonché informare e rendere consapevoli i primi di quanto sia importante proteggere il diritto alla riservatezza, propria e altrui, mediante una gestione selettiva e pertinente delle informazioni. Il nostro Istituto si è allineato, da tempo, al "Regolamento UE 2016/679", il cosiddetto "GDPR" (General Data Protection Regulation) e ha recepito il D. Lgs. 30 giugno 2003, n. 196. Al fine di garantire massima trasparenza infatti, al momento dell'iscrizione, la Scuola fornisce alle famiglie una "Informativa sul trattamento dei dati personali", ai sensi dell'art. 13 del citato D.Lgs. 196/2003 (Codice della privacy) e dell'art. 13 del Regolamento UE 679/2016 (GDPR), improntato ai principi di "liceità, correttezza, pertinenza, necessità e trasparenza, onde tutelare il diritto alla riservatezza, al decoro e alla reputazione della persona".

I dati personali sono trattati, sia con strumenti elettronici che cartacei, solo ed esclusivamente per le finalità istituzionali della Scuola. Il loro conferimento è obbligatorio per quanto attiene alle informazioni richieste dal modulo base dell'iscrizione, pena l'impossibilità di definire i procedimenti connessi all'iscrizione stessa dell'alunno/a, facoltativo per le informazioni supplementari. In calce trovano spazio i Diritti degli interessati in materia di accesso, rettifica, cancellazione, portabilità, opposizione e reclamo.

Alle famiglie vengono, inoltre, contestualmente forniti un "Modello di comunicazione dei dati necessari alla dematerializzazione dei rapporti scuola/famiglia" e specifica "Informativa per l'uso delle immagini" con annesso "Modello di autorizzazione", sempre ai sensi del D.Lgs. 196/2003 e del Regolamento UE 679/2016. Sebbene rientranti nel conferimento facoltativo di dati, dunque eccedenti rispetto i trattamenti istituzionali obbligatori, l'eventuale mancato conferimento delle richieste informazioni potrebbe comportare l'impossibilità per la Scuola di erogare efficacemente e in tutte le sue potenzialità il proprio servizio. Per quanto concerne nello specifico il trattamento di immagini (riprese fotografiche e cinematografiche in cui compaia l'immagine dell'alunno/a), il consenso prestato implica il loro utilizzo esclusivamente a fini di documentazione didattica, fermo restando la garanzia che l'immagine in questione sarà sempre rispettosa della dignità e della personalità del soggetto coinvolto. Analoga riflessione si applica per quanto riguarda la realizzazione da parte degli studenti di elaborati di qualsivoglia natura, in occasione della partecipazioni ad iniziative concorsuali interne o esterne, bandite dalla scuola o da essa sostenute. In tali casi

viene prodotta dalle famiglie specifica "Liberatoria" mediante la quale viene concessa alla scuola «una licenza di uso completa, a titolo gratuito e a tempo indeterminato per tutti gli utilizzi collegati alla suddetta iniziativa e su qualsiasi media e supporto».

Il consenso al trattamento include anche il passaggio del fascicolo dell'alunno ad una scuola differente affinché la scuola di destinazione, nel momento in cui l'alunno diventa suo frequentante, acceda e possa trattare i dati registrati nel fascicolo esistente; il fascicolo verrà storicizzato ed inviato dalla scuola di origine, che provvederà a cancellare i dati presenti nei suoi archivi.

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.

L'accesso ad Internet avviene con le credenziali ed è consentito solo ai docenti per fini legati alle proprie mansioni (registro elettronico, ricerca materiale didattico, ecc.).

L'accesso nei laboratori di Informatica e multimediale è consentito a docenti, studenti e personale esterno in occasione di corsi di formazione, ed avviene con immissione di credenziali. I PC dei laboratori richiedono l'autenticazione e sono utilizzabili solo con digitazione di specifiche credenziali. Gli studenti accedono sotto il controllo del docente e nel pieno rispetto delle norme di sicurezza, nella doppia accezione di safety e security.

Da un punto di vista tecnico, all'interno dell'Istituto esistono due Reti informatiche separate, una dedicata alla gestione amministrativa e l'altra alla didattica. Nell'Istituto sono presenti 36 laboratori di cui 11 di Informatica con 25 PC; da ciascuna delle postazioni gli studenti possono compiere tutte le operazioni previste dai programmi di studio dei corsi che si svolgono nel Laboratorio, utilizzare i software e le procedure installati sui PC, con collegamento ad internet; accedere ad Internet ed interagire con la postazione docente. In tutti i laboratori sono presenti stampanti e proiettori, in taluni casi la digital board. Tutte le postazioni vengono periodicamente controllate onde evitare affaticamento visivo e muscolare, guasti elettrici, rischi igienico-ambientali o di incendio. Le 56 aule didattiche sono provviste di digital boards collegate alla rete internet dell'Istituto. Altri dispositivi presenti sono 33 digital board (31 LIM), 60 tablet e 3 Flip e 1 Ledwall in altre aule dell'Istituto. Gli studenti inoltre, hanno a disposizione annualmente circa 100 dispositivi laptop in comodato d'uso.

3.3 - Strumenti di comunicazione online

Le tecnologie digitali sono in grado di ridefinire gli ambienti di apprendimento, supportando la comunicazione a scuola e facilitando un approccio sempre più collaborativo. L'uso degli strumenti di comunicazione online a scuola, al fianco di

quelli più tradizionali, ha l'obiettivo di rendere lo scambio comunicativo maggiormente interattivo e orizzontale. Tale uso segue obiettivi e regole precise correlati alle caratteristiche, funzionalità e potenzialità delle tecnologie digitali.

L'IIS Giua adotta da tempo vari strumenti di comunicazione online, sia per raggiungere target esterni, al fine di valorizzare e promuovere le attività portate avanti dall'Istituto trasmettendo all'esterno l'identità, i valori, l'idea di educazione fatte proprie dalla Scuola, sia per far circolare al suo interno, fra i diversi attori scolastici, informazioni di servizio o contenuti importanti. Per quanto riguarda, nello specifico, gli strumenti di comunicazione interna, la scuola adotta le seguenti modalità telematiche: - nella gestione delle relazioni scuola/famiglia, si fa ricorso al Registro elettronico, strumento principe della comunicazione in contesto scolastico, accessibile da entrambi gli utenti tramite credenziali personali. È possibile la prenotazione informatizzata dei colloqui con i docenti da parte dei genitori, nonché l'inoltro e la ricezione di documentazione riguardante la vita della scuola. In relazione a quest'ultimo aspetto, è assicurata alle famiglie, nel rispetto delle norme di riservatezza, l'informazione trasparente e tempestiva sul processo di apprendimento e sulla valutazione degli alunni effettuata nei diversi momenti del percorso scolastico. Nella gestione dei rapporti dirigenza/personale i canali comunicativi privilegiati sono la posta istituzionale e l'area riservata del Registro elettronico che i docenti si impegnano quotidianamente a controllare. La comunicazione docenti/alunni avviene attraverso aree dedicate del Registro elettronico, accessibili da entrambi tramite credenziali personali. È possibile condividere materiale didattico con i docenti e, anche in questo caso, avere accesso a informazioni in modo trasparente e tempestivo

La piattaforma Google consente di svolgere a distanza riunioni di carattere didattico e organizzativo e risponde ai necessari requisiti di sicurezza dei dati a garanzia della privacy, assicura un agevole svolgimento dell'attività sincrona e risulta fruibile da qualsiasi tipo di device. L'accesso al servizio avviene mediante credenziali personali.

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.

Il nostro Istituto è dotato di un regolamento sull'uso delle TIC e di una Netiquette che verranno poi allegate alla ePolicy. Nel regolamento sull'uso delle tecnologie vengono elencate le regole di utilizzo della strumentazione tecnologica della scuola, ovvero le azioni che docenti, personale scolastico e studenti/esse possono e non possono compiere quando si connettono alla Rete e/o accedono a un device. Tale regolamento prevede anche una parte sull'uso della strumentazione personale a scuola, sia nel caso del BYOD, qualora i docenti propongano ai propri studenti l'uso di device personali (tablet, PC o smartphone) in classe, ma anche regole per quanto riguarda la presenza degli smartphone a scuola, non a supporto delle attività didattiche. La PUA (Politica d'Uso Accettabile), verrà aggiornata e allegata all'ePolicy.

Nel regolamento gli studenti si impegnano a:

- utilizzare la rete nel modo corretto
- rispettare le consegne dei docenti
- non scaricare materiali e software senza autorizzazione
- non utilizzare unità removibili personali senza autorizzazione
- tenere spento lo smartphone al di fuori delle attività didattiche che ne prevedano l'utilizzo
- utilizzare lo smartphone esclusivamente previa autorizzazione del docente

I docenti si impegnano a:

- utilizzare la rete nel modo corretto
- non utilizzare device personali se non per uso didattico
- formare gli studenti all'uso della rete
- dare consegne chiare e definire gli obiettivi delle attività
- monitorare l'uso che gli studenti fanno delle tecnologie a scuola.

La legge 71 del 29 maggio 2017, chiede alle scuole di aggiornare il patto di corresponsabilità, per cui andrebbe inserito un punto specifico relativo all'uso della connessione Internet della scuola. La scuola dovrebbe informare che si farà carico di tutte le precauzioni necessarie per garantire agli/le studenti/esse l'accesso a materiale appropriato, ma che allo stesso tempo non può essere responsabile per l'accesso autonomo da parte degli/le studenti/esse a materiali inadeguati e potenzialmente dannosi trovati online.

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 incontri per la consultazione degli studenti/studentesse su indicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

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

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 e sulla protezione dei dati
- Organizzare incontri per la consultazione degli studenti/studentesse su indicazioni/regolamenti sull'uso dei dispositivi digitali personali
- Organizzare incontri per la consultazione dei genitori su indicazioni/regolamenti sull'uso dei dispositivi digitali personali
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della

protezione dei dati personali

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

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

4.1 - Sensibilizzazione e Prevenzione

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

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

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

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

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

La diffusione delle tecnologie digitali e dell'accesso alla Rete fra i più giovani è all'origine di profondi cambiamenti nelle dinamiche relazionali e in quelle identitarie: mutano linguaggi, modalità di comunicazione, abitudini e stili di vita, si offrono inedite potenzialità di crescita. Al tempo stesso, tuttavia, come già ampiamente dibattuto, questi nuovi e privilegiati strumenti di partecipazione portano in primo piano il

delicato tema della “sicurezza” e del comportamento sociale. Siamo, evidentemente, di fronte ad una realtà complessa, nella quale, accanto a nobili fini, trovano spazio contenuti e comportamenti potenzialmente dannosi, sfocianti talvolta in veri e propri reati, dal Cyberbullismo all’Hate speech, dalla Dipendenza da Internet ai Giochi online, dal Sexting al Grooming alla Pedopornografia online. Occorre, pertanto, promuovere nei ragazzi l’acquisizione delle necessarie competenze e capacità affinché possano adeguatamente proteggersi, utilizzare i nuovi media con consapevolezza, sfruttare le potenzialità delle tecnologie digitali e gestirne le implicazioni. La responsabilità dell’azione preventiva ed educativa coinvolge diverse agenzie formative, in primis la famiglia e la scuola. La necessità di supportare un uso positivo e consapevole delle TIC da parte dei più giovani, sia in un’ottica di tutela dai rischi potenziali che nella valorizzazione delle opportunità esistenti, pone entrambe di fronte alla sfida di riconsiderare la propria identità, il proprio ruolo educativo e le proprie risorse, oltre allo stato dei rapporti reciproci per un patto educativo da rinnovare costantemente.

Il nostro Istituto intende rafforzare la sua capacità di rispondere a questi nuovi bisogni attraverso strumenti e misure specifiche, dando una risposta il più possibile integrata, che trovi la sua espressione di indirizzo in procedure chiare di cui la Scuola dovrà dotarsi e che includano la collaborazione con la rete dei servizi locali (in primis la Polizia Postale). È opportuno, inoltre, che i docenti, nell’espletamento delle proprie funzioni di formatori ed educatori sappiano cogliere ogni opportunità per riflettere insieme agli alunni su tali rischi. Fondamentale monitorare costantemente le relazioni interne alla classe, onde individuare possibili situazioni di disagio ed intervenire tempestivamente, anche mediante il ricorso alle figure di sistema specializzate, nonchè allo Sportello di consulenza psicologica attivo da anni presso l'Istituto, per sostenere il singolo nelle situazioni di difficoltà personale e indirizzare il gruppo verso l’instaurazione di un clima positivo, di reciproca accettazione e rispetto, nelle situazioni di difficoltà socio-relazionale. Tale percorso interno potrà essere ulteriormente rinforzato dalla partecipazione a progetti e/o iniziative esterne coerenti con i temi sopra menzionati, cui la Scuola porrà particolare attenzione, selezionando eventi significativi promossi da Enti e/o Associazioni di comprovata affidabilità.

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).

In relazione ai casi più gravi, occorre precisare che per il nostro ordinamento l’imputabilità penale, ossia la responsabilità personale per i reati commessi, scatta al quattordicesimo anno. Se, dunque, il minore non ha compiuto i 14 anni, non risponde penalmente per l’evento, ma i genitori saranno tenuti al risarcimento del danno, per presunta “culpa in educando”, così come previsto dal Codice civile per i fatti commessi dal figlio. Eventuali responsabilità possono ricadere anche sulla Scuola, nel caso di comportamenti penalmente rilevanti verificatisi in tale contesto. È noto, infatti, che l’insegnante abbia un dovere di vigilanza e di conseguenza verrà addebitata, in caso di comportamento illecito del minore affidato, una colpa presunta, cioè una “culpa in vigilando”, come inadempimento dell’obbligo di sorveglianza sugli allievi. Da questa colpa/responsabilità si può essere liberati dimostrando di non aver potuto impedire il fatto. Esiste poi una “culpa in organizzando”, quando la Scuola non mette in atto le azioni previste per la prevenzione e gestione del fenomeno, così come sancito dalla normativa vigente. In ottemperanza alla normativa vigente che invita, tra l’altro, a pianificare interventi di natura preventiva ed educativa e non solo sanzionatoria.

La nostra Scuola si avvale, come previsto dalla normativa, della collaborazione di una figura preposta, individuata fra i docenti, di due Referenti per il Bullismo e il Cyberbullismo cui spetta il compito di coordinare le iniziative di prevenzione e contrasto del fenomeno, in sinergia con le Forze di Polizia, le Associazioni e i centri di aggregazione giovanile presenti sul territorio. Il Referente, inoltre, svolge compito di supporto al Dirigente scolastico in occasione della revisione di Regolamenti, atti e documenti d'Istituto, con particolare riferimento alle sezioni inerenti i temi del bullismo/cyberbullismo. Determinante il supporto dell'Animatore digitale nella promozione e diffusione di buone pratiche, nonché della comunità educante tutta, quotidianamente impegnata nell'intessere un costruttivo dialogo con i propri studenti e, quindi, sensibile a coglierne eventuali manifestazioni di disagio.

4.3 - Hate speech: che cos'è e come prevenirlo

Il fenomeno di "incitamento all'odio" o "discorso d'odio", indica discorsi (post, immagini, commenti etc.) e pratiche (non solo online) che esprimono odio e intolleranza verso un gruppo o una persona (identificate come appartenente a un gruppo o categoria) e che rischiano di provocare reazioni violente, a catena. Più ampiamente il termine "hate speech" indica un'offesa fondata su una qualsiasi discriminazione (razziale, etnica, religiosa, di genere o di orientamento sessuale, di disabilità, eccetera) ai danni di una persona o di un gruppo.

Tale fenomeno, purtroppo, è sempre più diffuso ed estremamente importante affrontarlo anche a livello educativo e scolastico con l'obiettivo di:

- fornire agli studenti gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di hate speech, in particolare legati alla razza, al genere, all'orientamento sessuale, alla disabilità;
- promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network;
- favorire una presa di parola consapevole e costruttiva da parte dei giovani.

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere in relazione a questa problematica.

La pratica dell'hate speech si è fortemente diffusa e rafforzata negli ultimi anni soprattutto attraverso l'uso della Rete, alimentando un dibattito tanto attuale quanto controverso poiché afferente il delicato tema della libertà di espressione. Scenario privilegiato sono diventati i Social network, dove non è difficile e infrequente imbattersi in forme di incitamento all'odio particolarmente violente, tanto più che

presunti impunità e anonimato abbassano ogni remora etica. Data la viralità del fenomeno, diventa molto importante sensibilizzare le nuove generazioni e attuare interventi di natura preventiva partendo proprio dal contesto scolastico. Incentivare nei giovani la piena partecipazione alla vita, in forma attiva e costruttiva, è la missione che ciascun docente della nostra scuola, indipendentemente dall'insegnamento impartito, abbraccia. Si tratta di fornire ai ragazzi gli strumenti per "appropriarsi" della realtà che li circonda, nella consapevolezza che tale possesso, acquisizione, passi proprio attraverso un uso sapiente, virtuoso e costruttivo della parola da promuovere quotidianamente, dentro e fuori dall'aula. La finalità è promuovere un clima di collaborazione tra pari e non, riflettere sulla libertà di espressione, sul labile confine tra rispetto e offesa, utilizzare il linguaggio mediatico come veicolo di inclusione e non di vessazione.

4.4 - Dipendenza da Internet e gioco online

La Dipendenza da Internet fa riferimento all'utilizzo eccessivo e incontrollato di Internet che, al pari di altri comportamenti patologici/dipendenze, può causare o essere associato a isolamento sociale, sintomi da astinenza, problematiche a livello scolastico e irrefrenabile voglia di utilizzo della Rete.

L'istituto è intenzionato a promuovere azioni di prevenzione attraverso percorsi sul benessere digitale?

Il fenomeno si connota per un progressivo e totale assorbimento del soggetto alla rete con drastiche ripercussioni sul suo stile di vita: l'attività domina patologicamente i suoi pensieri ed il suo comportamento, assumendo un valore primario tra tutti i suoi interessi. Spesso, inoltre, il trascorrere del tempo online in termini disfunzionali è scandito dal gioco virtuale che può assumere le forme della Dipendenza dal gioco online. Data la natura e le sue implicazioni, la IAD rappresenta una questione importante per la comunità scolastica che ha il dovere di cogliere il fenomeno, sensibilizzare e prevenire fornendo agli studenti gli strumenti e le competenze affinché maturino adeguata consapevolezza dei rischi legati all'iperconnessione. Tale presa d'atto non significa demonizzare la Rete: indubbi sono, infatti, i vantaggi derivanti da un suo uso accorto e responsabile. Il nostro istituto è un convinto assertore del "benessere digitale", inteso come capacità di creare e mantenere una relazione sana con la tecnologia che ha certamente modificato gli ambienti in cui si vive e opera e che ha avuto e ha un impatto significativo sulla qualità della vita. Occorre, pertanto, riflettere con gli studenti sulle potenzialità insite nella tecnologia e su come poterla gestire affinché diventi strumento per raggiungere i propri obiettivi e non sia solo

distrazione o addirittura ostacolo. Ciò diventa possibile in maniera diretta, attraverso specifiche dissertazioni sul tema, ma anche implicitamente, integrando la tecnologia nella didattica e mostrandone un impiego funzionale.

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.

All'origine del fenomeno vi sono varie motivazioni, dalla semplice e alquanto superficiale ammissione di goliardia che rivela totale assenza di consapevolezza rispetto all'entità del fenomeno e alle sue possibili conseguenze, sino ad arrivare alle forme estreme del ricatto e della vendetta, il cosiddetto "revenge porn", che configurano veri e propri reati. Ma a prescindere dalla sua genesi, gli effetti di una simile illecita diffusione sono ugualmente devastanti. La presa di coscienza della pervasività con cui si diffondono i contenuti condivisi, la cui trasmissione diventa incontrollabile, della loro giacenza in Rete per un tempo teoricamente illimitato, unitamente al doloroso, incolmabile e annichilente disagio legato alla percezione della propria fiducia tradita dal destinatario, generano profondi turbamenti, capaci di annientare emotivamente e socialmente la vittima. La problematica del sexting va, tuttavia, inquadrata in uno scenario più ampio. Essa è riconducibile ad una scarsa educazione emotiva e sessuale oltre che ad una assenza di competenza digitale per quanto attiene al modo in cui i giovani vivono la propria sessualità e la propria immagine online, il loro desiderio di esprimersi e affermare se stessi. Fondamentale diventa, quindi, in ambito scolastico, integrare il curriculum con temi legati all'affettività, alla sessualità e alla differenza di genere, e, contestualmente, portare avanti un percorso di educazione digitale che comprenda lo sviluppo di competenze quali la tutela della propria privacy, la gestione dell'immagine e dell'identità online, la capacità di vivere in modo sano le proprie relazioni in Rete.

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.

Il miglior modo per prevenire casi di adescamento online dovrebbe essere quello di accompagnare ragazze e ragazzi in un percorso di educazione, anche digitale, all'affettività e alla sessualità. Ciò aiuterebbe a renderli più sicuri emotivamente e pronti ad affrontare eventuali situazioni a rischio, imparando innanzitutto a gestire le proprie emozioni, il rapporto con il proprio corpo e con gli altri. È molto importante, inoltre, che ragazzi e ragazze sappiano a chi rivolgersi in caso di problemi, anche quando pensano di aver fatto un errore, si vergognano o si sentono in colpa. Gli adulti coinvolti, genitori e docenti, devono essere un punto di riferimento per il minore che deve potersi fidare di loro e non sentirsi mai giudicato, ma compreso e ascoltato. Affinché ciò avvenga è necessario tenere sempre aperto un canale di comunicazione con loro sui temi dell'affettività, del digitale e della sessualità. È quanto si impegna a fare la nostra scuola mediante l'attivazione di uno Sportello di consulenza psicologica, a disposizione di studenti e genitori e promuovendo la conoscenza del servizio di Helpline predisposto da Generazioni Connesse, dedicato ai giovani o ai loro familiari che possono chattare, inviare e-mail o parlare al telefono con professionisti qualificati relativamente a dubbi, domande o problemi legati all'uso delle nuove tecnologie digitali e alla sicurezza online. Si tratta, evidentemente, di una problematica molto delicata da gestire, che richiede l'immediato intervento della Polizia Postale e delle Comunicazioni.

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 pedopornografia dopo l'avvento di Internet, con l'evoluzione e la moltiplicazione dei "luoghi" virtuali, il cambiamento costante delle stesse tecnologie digitali, ha radicalmente mutato il modo in cui il materiale pedopornografico viene prodotto e diffuso, contribuendo ad un aumento della sua disponibilità e dei canali di diffusione.

L'abuso sessuale online rappresenta, dunque, una particolare declinazione dell'abuso sessuale su bambini/e, ragazzi/e, la cui caratteristica fondante è il ruolo ricoperto dalle tecnologie digitali, le quali diventano il mezzo principale attraverso cui l'abuso viene perpetrato, documentato e diffuso in Rete con immagini e/o video. Le dinamiche attraverso cui l'abuso sessuale online si manifesta producono effetti sulle vittime che si aggiungono e moltiplicano a quelli associati all'abuso sessuale. Studi in materia dimostrano, inoltre, come l'utilizzo di materiale pedopornografico possa essere propedeutico all'abuso sessuale agito ed è quindi fondamentale intervenire, in termini preventivi, per ridurre l'incidenza di tale eventualità. Fermo restando la possibilità/necessità di confronto con l'adulto di riferimento ogni qualvolta un contenuto online susciti disagio, la Scuola deve adoperarsi attivamente, agendo in sinergia con le famiglie, affinché i ragazzi acquisiscano le necessarie competenze in grado di orientarli e guidarli nelle loro scelte, anche online. Per questo motivo, un canale comunicativo sempre vigile, un'attenzione ai temi dell'affettività e delle relazioni mediate dal digitale, una seria e strutturata riflessione sul tema dell'affidabilità delle fonti online e, più in generale dell'educazione digitale, concepiti come parte integrante del curriculum d'Istituto, nonché la possibilità di confronto con esperti qualificati, rivestono un ruolo fondamentale nella comprensione e gestione di un così delicato tema.

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 di formazione all'utilizzo sicuro e consapevole di Internet e delle tecnologie digitali integrando lo svolgimento della didattica e assicurando la partecipazione attiva

degli studenti/studentesse.

- Promuovere incontri e laboratori per studenti e studentesse dedicati all' Educazione Civica Digitale.
- Organizzare uno o più incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/le studenti/studentesse.
- Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/le studenti/studentesse.
- **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.
- Organizzare uno o più incontri di formazione all'utilizzo sicuro e consapevole di Internet e delle tecnologie digitali integrando lo svolgimento della didattica e assicurando la partecipazione attiva degli studenti/studentesse.
- Promuovere incontri e laboratori per studenti e studentesse dedicati all' Educazione Civica Digitale.
- Organizzare uno o più incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/le studenti/studentesse.
- Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/le studenti/studentesse.
- Organizzare uno o più eventi e/o dibattiti in momenti extra-scolastici, sui temi della diversità e sull'inclusione rivolti a genitori, studenti/studentesse e personale della scuola.
- 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.

La nostra istituzione scolastica ha attivato il Protocollo per contrastare le azioni di bullismo e cyberbullismo, approvato in Consiglio di Istituto nel corrente anno scolastico.

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).

Nel caso si assista ad un episodio tra quelli di cui sopra, si deve condividere immediatamente quanto osservato con il referente per il bullismo e il cyberbullismo (e/o il referente indicato nell'ePolicy), valutando insieme le possibili strategie di intervento. Nella nostra scuola è attivo il PROTOCOLLO DI INTERVENTO nei casi BULLISMO E CYBERBULLISMO che contiene gli strumenti a disposizione di studenti/esse per le segnalazioni. In particolare:

ALLEGATO 1 (scheda di prima segnalazione)

ALLEGATO 2 (scheda di valutazione approfondita)

ALLEGATO 3 (scheda di monitoraggio)

ALLEGATO 4 (modello per la segnalazione reclamo in materia di cyberbullismo al Garante per la protezione dei dati personali).

5.3. - Gli attori sul territorio

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

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

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

- **Comitato Regionale Unicef**: laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.

- **Co.Re.Com. (Comitato Regionale per le Comunicazioni):** svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare attenzione alla tutela dei minori.
- **Ufficio Scolastico Regionale:** supporta le scuole in attività di prevenzione ed anche nella segnalazione di comportamenti a rischio correlati all'uso di Internet.
- **Polizia Postale e delle Comunicazioni:** accoglie tutte le segnalazioni relative a comportamenti a rischio nell'utilizzo della Rete e che includono gli estremi del reato.
- **Aziende Sanitarie Locali:** forniscono supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in Rete. In alcune regioni, come il Lazio e la Lombardia, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da Internet e alle situazioni di rischio correlate.
- **Garante Regionale per l'Infanzia e l'Adolescenza e Difensore Civico:** segnalano all'Autorità Giudiziaria e ai Servizi Sociali competenti; accolgono le segnalazioni di presunti abusi e forniscono informazioni sulle modalità di tutela e di esercizio dei diritti dei minori vittime. Segnalano alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.
- **Tribunale per i Minorenni:** segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

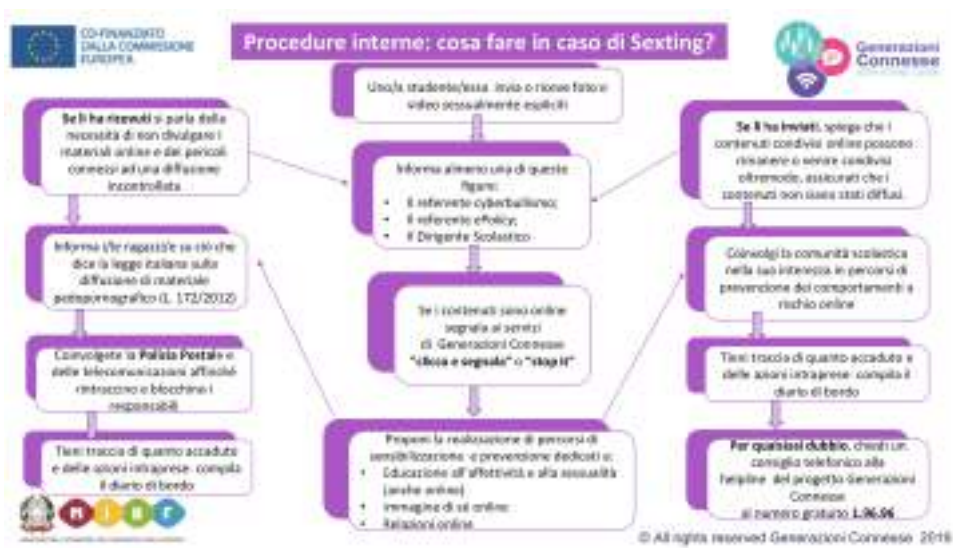
5.4. - Allegati con le procedure

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

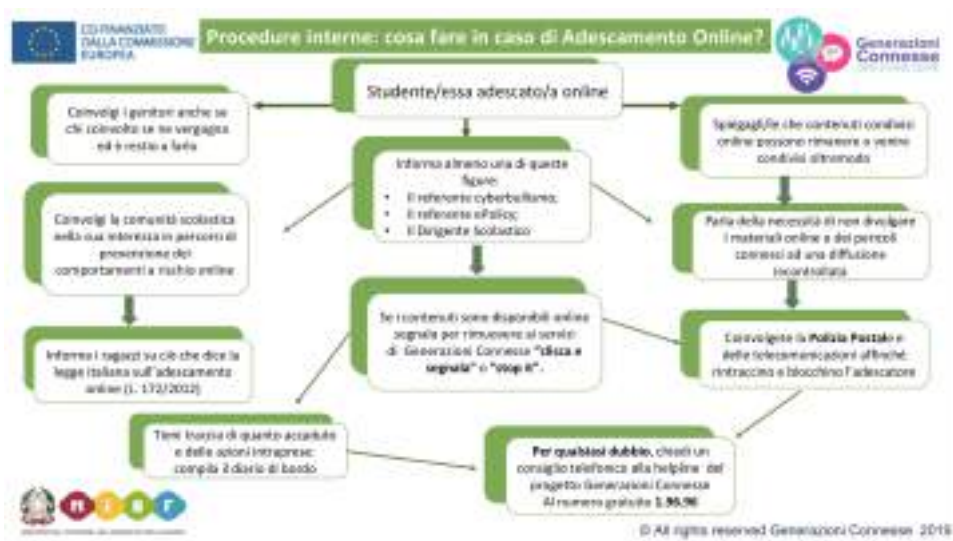




Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



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



Altri allegati

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

<https://www.giua.edu.it/prevenzione-bullismo-e-cyberbullismo/>

Il nostro piano d'azioni

Non è prevista nessuna azione.

