Documento di ePolicy

CSTF01000C

ITI "MONACO" COSENZA

VIA GIULIA 9 - 87100 - COSENZA - COSENZA (CS)

Fiorangela D'Ippolito

Capitolo 1 - Introduzione al documento di ePolicy

1.1 - Scopo dell'ePolicy

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

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

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

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

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

Argomenti del Documento

Perché è importante dotarsi di una E-policy?

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

all'uso di Internet.

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

1.2 - Ruoli e responsabilità

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

I soggetti coinvolti in tale processo pertanto saranno: il Dirigente Scolastico, l'Animatore digitale, il Team ed il Referente del bullismo e del cyderbullismo, i docenti, gli studenti e le loro famiglie.

Nella promozione dell'uso consapevole della rete il Dirigente Scolastico deve:

- Garantire la corretta formazione del personale scolastico sulle tematiche relative all'uso sicuro e consapevole di Internet e della rete.
- Garantire una formazione adeguata del personale docente relativo all'uso delle TIC nella didattica.
- Garantire che le modalità di utilizzo corretto e sicuro delle TIC e di Internet siano integrate nel curriculum di studio e nelle attività didattiche ed educative delle classi.
- Garantire l'esistenza di un sistema in grado di consentire il monitoraggio e il controllo interno della sicurezza on-line.
- Seguire le procedure previste dalle norme in caso di reclami o attribuzione di responsabilità al personale scolastico in relazione a incidenti occorsi agli alunni nell'utilizzo delle TIC a scuola.

L'Animatore digitale, supportato dal Team dell'innovazione, deve:

- Stimolare la formazione interna all'istituzione negli ambiti di sviluppo della "scuola digitale" e fornire consulenza e informazioni al personale in relazione ai rischi on-line e alle misure di prevenzione e gestione degli stessi.
- Monitorare e rilevare le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola, nonché proporre la revisione delle politiche dell'istituzione con l'individuazione di soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola.
- Assicurare che gli utenti possano accedere alla rete della scuola solo tramite password applicate e regolarmente cambiate e curare la manutenzione e lo

sviluppo del sito web della scuola per scopi istituzionali e consentiti (istruzione e formazione).
- Coinvolgere la comunità scolastica (alunni, genitori e altri attori del territorio) nella partecipazione ad attività e progetti attinenti alla "scuola digitale".

Il Referente del bullismo e cyberbullismo deve:

- Coordinare e promuovere iniziative specifiche per la prevenzione e il contrasto del bullismo e cyberbullismo (può avvalersi della collaborazione delle Forze di polizia, Associazioni e centri di aggregazione giovanile del terrotorio).
- Coinvolgere (ove possibile), con progetti e percorsi formativi ad hoc, studenti, colleghi e genitori.

I Docenti devono:

- Informarsi/aggiornarsi sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di Internet e sulla politica di sicurezza adottata dalla scuola, rispettandone il regolamento.
- Garantire che gli alunni comprendano e seguano le regole per prevenire e contrastare l'utilizzo scorretto e pericoloso delle TIC e di Internet.
- Segnalare qualsiasi problema o proposta di carattere tecnico-organizzativo ovvero esigenza di carattere informativo, all'Animatore digitale ai fini della ricerca di soluzioni metodologiche e tecnologiche innovative da diffondere nella scuola e di un aggiornamento della politica adottata in materia di prevenzione e gestione dei rischi nell'uso delle TIC;
- Segnalare al Dirigente scolastico e ai genitori qualsiasi abuso rilevato a scuola nei confronti degli alunni in relazione all'utilizzo delle tecnologie digitali o di Internet, per l'adozione delle procedure previste dalle norme.

Gli Alunni devono:

- Essere responsabili, in relazione al proprio grado di maturità e di apprendimento, nell'utilizzo dei sistemi delle tecnologie digitali in conformità con quanto richiesto dai docenti.
- Avere una buona comprensione delle potenzialità offerte dalle TIC per la ricerca di contenuti e materiali, ma anche della necessità di evitare il plagio e rispettare i diritti d'autore.
- Comprendere l'importanza di adottare buone pratiche di sicurezza on-line quando si utilizzano le tecnologie digitali per non correre rischi.
- Adottare condotte rispettose degli altri anche quando si comunica in rete.
- Esprimere domande o difficoltà o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o di Internet ai docenti e ai genitori.

I Genitori devono:

- Sostenere la linea di condotta della scuola adottata nei confronti dell'utilizzo delle TIC nella didattica;

- Seguire gli alunni nello studio a casa adottando i suggerimenti e le condizioni d'uso delle TIC indicate dai docenti.
- Relazionarsi in modo costruttivo con le docenti sulle linee educative che riguardano le TIC e la Rete e comunicare con loro circa i problemi rilevati quando i figli non usano responsabilmente le tecnologie digitali o Internet.
- Fissare delle regole per l'utilizzo del computer e tenere sotto controllo l'uso che i figli fanno di Internet e dello smartphone in generale.

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).

Dotarsi di un'informativa sintetica sull'ePolicy comprensiva delle procedure di segnalazione da condividere con tutte le figure che operano con studenti e studentesse, significa non solo tutelare questi ultimi e la scuola stessa, ma anche porre in essere nuove modalità per rilevare, limitare e contrastare possibili pericoli legati a condotte educative non professionali. Tale documento chiarisce il sistema di azioni e le procedure di segnalazione da seguire, valide anche per i professionisti e le organizzazioni esterne, finalizzate a rilevare e gestire le problematiche connesse ad un uso non consapevole delle tecnologie digitali. In questo modo, si facilita la presa in carico da parte della scuola, qualora si verifichino problematiche derivanti da un

utilizzo non corretto delle tecnologie digitali. Tale documento, inoltre, permette di tutelare ragazzi e ragazze da comportamenti potenzialmente rischiosi messi in atto da soggetti esterni alla scuola e che si trovano ad operare all'interno dell'Istituto. L'informativa deve essere condivisa e sottoscritta nella stipula di eventuali contratti con personale e associazioni esterne: le figure professionali e le organizzazioni coinvolte in progetti, laboratori e attività devono, in altri termini, prendere visione di tutti i documenti proposti dall'Istituto e sottoscriverli preliminarmente all'avvio dei programmi con gli studenti e le studentesse, in classe o fuori.

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

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

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

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

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

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

1.5 - Gestione delle infrazioni alla ePolicy

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

Le infrazioni all'E-Policy possono essere rilevate da docenti/ATA nell'esercizio delle proprie funzioni, oppure possono essere segnalate da alunni e/o genitori a docenti e/o ATA. Nel momento stesso in cui qualunque attore della comunità scolastica venga a conoscenza di una infrazione nell'utilizzo delle TIC e di internet, strumenti messi a disposizione degli alunni a fini puramente didattici, ha l'obbligo di comunicarlo con la massima urgenza al D.S. perché adotti le misure necessarie.

Il procedimento disciplinare nei confronti dell'alunno sarà avviato dopo aver valutato le seguenti ipotesi:

- Il fatto non costituisce reato o ipotizza un reato a querela di parte.

Il Dirigente Scolastico, informa tempestivamente i genitori (o chi esercita la responsabilità genitoriale), e attiva adeguate azioni di carattere educativo mediante lo svolgimento di attività di natura sociale, culturale e in generale a vantaggio della comunità scolastica.

- Il fatto costituisce reato

Il Dirigente Scolastico sporge subito denuncia per iscritto ad un organo di polizia o all'autorità giudiziaria (Questura, Carabinieri ecc.), anche quando non sia individuata la persona alla quale il reato è attribuito. (art 331 cpp).

All'interno della procedura disciplinare, si inserisce una parte specifica per gli episodi di bullismo e cyberbullismo, riportata nel Vademecum "Bullismo e Cyberbullismo" pubblicato sul sito web della scuola.

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 Interno del nostro Istituto è stato integrato con una sezione relativa alla nomina del referente per le attività di prevenzione e di contrasto del bullismo e del

cyberbullismo; è stata aggiunta una sezione relativa ai comportamenti sanzionabili e ai provvedimenti riguardanti l'uso non corretto della strumentazione personale e di qualsiasi dispositivo elettronico durante l'orario scolastico. Inoltre, sono state inserite le procedure operative da adottare negli eventuali casi di bullismo e cyberbullismo.

1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

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

Il monitoraggio e l'eventuale aggiornamento dell' E-Policy sarà curato dal Dirigente Scolastico con la collaborazione dell'Animatore digitale, del Team e del Referente al bullismo e cyberbullismo. Avrà il fine di rilevare la situazione iniziale delle classi e gli esiti a fine anno, in relazione all'uso sicuro e responsabile delle tecnologie digitali e di Internet.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

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

Azioni da svolgere nei prossimi 3 anni:

- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto agli studenti.

- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai genitori.

Capitolo 2 - Formazione e curricolo

2.1. Curricolo sulle competenze digitali per gli studenti

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

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

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

L'Istituto Tecnico Industriale "A. Monaco" consapevole che l'attenzione ai bisogni ed alle esigenze di ciascuno, che la valorizzazione dei talenti e del merito, la centralità della persona e la formazione integrale, rappresentano i cardini imprescindibili dell'azione educativa, predispone un "Progetto di Scuola Digitale" che, attraverso le sue azioni, interviene fattivamente a dare qualità alla preparazione degli alunni e crescita culturale al territorio.

Il nostro Istituto investe da tempo sull'uso didattico delle TIC e di Internet. Con l'utilizzo della piattaforma di e-learning, mira ad ottimizzare l'attività didattica, mediante la realizzazione di classi virtuali che favoriscono la collaborazione, la condivisione di materiali didattici, lo svolgimento di esercizi o verifiche.

La piattaforma fornisce un modo semplice e sicuro per supportare l'apprendimento e aiutare gli studenti a sviluppare importanti competenze on-line.

L'Animatore digitale e i docenti del Team di innovazione digitale garantiscono il necessario sostegno, progettando e realizzando attività di alfabetizzazione digitale rivolte agli studenti dell'Istituto, anche attraverso il coinvolgimento di quelli più esperti. Tali attività sono finalizzate all'acquisizione delle abilità di base per l'utilizzo degli strumenti digitali e, in particolare, delle piattaforme in dotazione alla Scuola per le attività didattiche.

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.

Per favorire l'implementazione, l'organizzazione, la presenza e l'uso consapevole e sistematico delle risorse e delle tecnologie digitali, la nostra scuola ha fissato un piano di azioni ritenute prioritarie e percorribili, riferite ai tre ambiti progettuali assegnati dal PNSD all'animatore digitale.

L'intero piano, presentato in tre momenti temporali, prevede i seguenti interventi relativi alla formazione interna:

- Creazione e mantenimento di uno sportello permanente di assistenza ai docenti (anche attraverso l'utilizzo di classi virtuali)
- Partecipazione alla rete territoriale e Nazionale Animatori Digitali
- Formazione docenti sulla piattaforma Google Suite
- Formazione per l'uso di applicazioni utili per l'inclusione
- Formazione sull'utilizzo della piattaforma www.collegioonline.it
- Corso di formazione ROBO-TEACH

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

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

L'Istituto Tecnico Industriale "A. Monaco" si avvale della figura dell'Animatore digitale che, con il Dirigente Scolastico e il D.S.G.A., collabora per raggiungere gli obiettivi di innovazione del PNSD nella scuola. Inoltre, la scuola ha attivato la figura del Referente d'Istituto per le attività di prevenzione e contrasto al bullismo e al cyberbullismo (L.107/2015).

Si propone, comunque, la formazione di tutti i docenti sull'uso consapevole e sicuro di Internet e sui rischi della rete. Il percorso di formazione dei docenti sarà permanente e in relazione all'evoluzione rapida delle tecnologie e delle modalità di comunicazione a cui accedono in maniera costante ed autonoma i ragazzi. Potrà prevedere momenti di autoaggiornamento e di formazione personale o collettiva, ma in futuro la scuola supporterà la formazione attraverso corsi interni o esterni, mediante seminari, conferenze e dibattiti. Non si escluderà la formazione a distanza né la partecipazione ad iniziative al di fuori della programmazione d'Istituto.

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.

La scuola, inoltre, si propone di sensibilizzare tutti gli attori educanti sui temi della sicurezza online mediante l'organizzazione di incontri aperti alle famiglie e agli studenti con enti esterni, come la Polizia Postale, e momenti di confronto e discussione con esperti sui rischi derivanti da un uso inappropriato delle tecnologie digitali e di Internet.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2023/2024)

- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare incontri con esperti per i docenti sulle competenze digitali.
- Organizzare incontri con esperti per i genitori sull'educazione alla cittadinanza digitale.

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

- Coinvolgere una rappresentanza dei genitori per individuare i temi di maggiore interesse nell'ambito dell'educazione alla cittadinanza digitale.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare incontri con esperti per i docenti sulle competenze digitali.

- Organizzare incontri con esperti per i genitori sull'educazione alla cittadinanza digitale.

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

3.1 - Protezione dei dati personali

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

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

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

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

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

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

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

Per dato personale si intende qualsiasi informazione riguardante una persona fisica identificata o identificabile. In particolare, si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con un nome, un numero d'identificazione, con dati relativi all'ubicazione, con un identificativo online, ecc. riferiti a uno o più elementi caratteristici della sua identità fisica, psichica, economica, culturale, ecc. e che possono fornire informazioni circa il suo stile di vita, le sue abitudini, le sue relazioni, il suo stato di salute, la sua situazione economica, e così via. Gli istituti scolastici hanno la possibilità di trattare i dati personali degli alunni e di tutto il personale scolastico, necessari al perseguimento di finalità istituzionali o quelli previsti dalla normativa vigente: per questi, le scuole non sono tenute a chiedere il consenso agli alunni e alle famiglie. Altri dati, invece, richiedono espressamente il consenso al trattamento dei dati personali. L'Istituto Tecnico Industriale "A. Monaco" è da sempre impegnato nella tutela della privacy degli utenti con il Regolamento d'Istituto e con il Patto di corresponsabilità.

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.

In ottemperanza a quanto stabilito dall'art. 2 della Dichiarazione dei diritti di Internet, elaborata dalla Commissione per i diritti e i doveri in Internet, costituita presso la Camera dei Deputati il 27 ottobre 2014, l'Istituto si è dotato di un software dedicato al controllo di tutti gli accessi in Internet dai dispositivi scolastici e ha vietato l'uso dei dispositivi personali, se non espressamente autorizzati dai docenti per fini esclusivamente didattici.

Gli studenti si impegnano a:

- non scaricare materiali e software senza autorizzazione;
- utilizzare la rete nel modo corretto;
- seguire e rispettare le indicazioni dei docenti;
- non utilizzare unità rimovibili personali senza autorizzazione;
- segnalare immediatamente materiali inadeguati ai propri insegnanti.
- durante le lezioni in presenza, tenere spento lo smartphone durante le attività didattiche che non prevedono espressamente l'utilizzo di supporti digitali, ad eccezione di conclamate motivazioni in materia di misure compensative di bisogno educativo speciale (autorizzate dal docente) o in momenti di classe capovolta (anche in aula) con finalità esclusiva alla didattica, limitatamente alla

consegna da svolgere;
- sono vietate registrazioni audio e video di quanto accade durante la lezione, ed è vietato anche condividere i link delle lezioni per evitare di invitare in chiamata estranei e disturbatori.

I docenti si impegnano a:

- utilizzare la rete nel modo corretto;
- 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.

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.

Lo sviluppo della tecnologia permette una più forte e duratura diffusione delle TIC all'interno delle classi, sia in presenza, sia in classe virtuale. Modificare l'ambiente dell'apprendimento comporta però un ripensamento della lezione che così passa da una "classica lezione frontale" ad una interattiva e coinvolgente che richiede al docente di modificare la sua metodologia e l'approccio comunicativo con gli studenti. La lezione digitale può essere definita tale, non solo perché si ha il collegamento in Internet e si utilizzano programmi e software applicativi, ma soprattutto perché vengono utilizzati in classe o durante la didattica a distanza per le lezioni quotidiane. Ciò richiede al docente una rimodulazione della progettazione dello spazio e delle nuove dinamiche che si stabiliscono andando a modificare la prassi comunicativa della classe e, quindi, il rapporto didattico tra il docente ed il discente, tra i docenti e tra gli

studenti. Lasciando entrare, appunto, nell'ambiente di apprendimento, eventualmente, ove se ne creasse la possibilità, soggetti esterni (soggetti nella rete o progettisti e produttore dei vari software didattici). Il Dirigente Scolastico e il personale che ha il compito di gestire le pagine del sito dell'Istituto, hanno la responsabilità di garantire che il contenuto pubblicato sia adeguato, attento ed accurato. Lo strumento di comunicazione interna utilizzato dall'Istituto è il registro elettronico (Axios) e software applicativi e piattaforme di lavoro collaborativo e condiviso (GMail, Classroom, Google Meet, ecc. della piattaforma G-Suite for Education). Il registro elettronico permette all'Istituto di gestire la comunicazione con le famiglie, le quali attraverso di esso possono visualizzare molte informazioni utili, interagendo con la scuola, su:

- andamento scolastico: assenze, argomenti lezioni e compiti, note disciplinari;
- risultati scolastici: voti, giudizi, documenti di valutazione;
- prenotazioni colloqui individuali;
- agenda eventi e scadenze;
- comunicazione varie sia di classe che individuali.

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.

Già dall'anno scolastico 2019/20 secondo le disposizioni del nuovo Patto educativo di Corresponsabilità, votato dal Collegio docenti e dal Consiglio d'Istituto nel 2019, gli studenti rispettano tassativamente in tutta l'area scolastica il divieto d'uso dei telefoni cellulari (Dir. Min. 15/03/07) e di qualsiasi altra apparecchiatura tecnologica per registrare immagini, sia statiche (fotografie), sia dinamiche (video

filmati), voci o suoni (tali azioni si configurano come violazione della privacy secondo il D. L. 30/06/2003).

E' altresì vietato l'uso dei telefoni cellulari e di qualsiasi altra apparecchiatura tecnologica per comunicare con l'esterno e/o trasmettere o ricevere messaggi, salvo casi di necessità su valutazione e autorizzazione del docente per gli studenti.

Resta la responsabilità deontologica e professionale del Dirigente, dei docenti e del personale ATA che hanno il dovere di vigilare sui comportamenti degli studenti e delle studentesse e di segnalare eventuali infrazioni suscettibili di sanzioni disciplinari.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2023/2024).

- 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.

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

- Organizzare incontri per la consultazione degli studenti/studentesse su indicazioni/regolamenti sull'uso dei dispositivi digitali personali
- Organizzare uno o più eventi o attività volti a formare 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.*

L'Istituto "A. Monaco ritiene indispensabili gli strumenti di sensibilizzazione e prevenzione.
Attraverso la "Sensibilizzazione" punta ad informare, ma soprattutto ad educare, alla consapevolezza e alla riflessione sulle seguenti tematiche:

- Uso o abuso di internet.

- Quanto sono dipendente dallo smartphone, che uso ne faccio, per quante ore nell'arco della giornata, riesco a darmi delle regole?
- Come la rete ha modificato il mio modo di comunicare e di pormi in relazione con l'altro; i gruppi whatsapp, la messaggistica sostituiscono il linguaggio verbale e non verbale?
- Quanto sono consapevole dei pericoli della rete, cosa penso di sapere, come penso di evitarli

Mediante la "Prevenzione" oltre a promuovere le competenze previste dal curriculo digitale un accento particolare viene dato:

- Alla conoscenza dell'importanza di tutelare la propria privacy e quella degli altri (dati sensibili, password, foto, video) e dell'implicazioni legali in caso di trasgressione.
- Alla conoscenza delle regole o norme etiche da tenere in mente quando si naviga in rete, quando si pubblica e/o si condivide un contenuto.
- Alla riflessione di come sia possibile dietro uno schermo, protetti dall'anonimato, infrangere con facilità tali norme, essere vittime o artefici di azioni lesive e offensive della propria e altrui persona.

4.2 - Cyberbullismo: che cos'è e come prevenirlo

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

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

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

- formazione del personale scolastico, prevedendo la partecipazione di un proprio referente per ogni autonomia scolastica;
- sviluppo delle competenze digitali, tra gli obiettivi formativi prioritari (L.107/2015);

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

Il Parlamento italiano ha approvato il 18 maggio 2017 la Legge 71/2017, una legge a tutela dei minori per la prevenzione e il contrasto al cyberbullismo che prevede misure prevalentemente a carattere educativo/rieducativo.

Come previsto dalla normativa, l'ITI "A. Monaco" ha nominato un referente con il compito di coordinare le iniziative di prevenzione e di contrasto al cyberbullismo e stilato un Vademecum, consultabile sul sito della scuola, che vuole essere una guida operativa finalizzata alla diffusione di strumenti conoscitivi sulle attività di prevenzione del fenomeno del cyberbullismo per tutta comunità scolastica.

Le strategie messe in atto dall'Istituto, per prevenire atti riconducibili ad atteggiamenti di cyberbullismo, si muovono nella direzione di creare un clima di fiducia, di stima e di accoglienza all'interno della scuola. I casi accertati di cyberbullismo possono essere segnalati attraverso le procedure attivate dall'Istituto. Qualora i fatti venissero accertati, lo stesso, si avvale del proprio regolamento al fine di sanzionare i colpevoli.

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.

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

- 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.

4.4 - Dipendenza da Internet e gioco online

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

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

benessere digitale?

La S.I.I.Pa.C., la Società Italiana Intervento Patologie Compulsive, definisce la dipendenza da Internet come progressivo e totale assorbimento del soggetto alla Rete. Di seguito alcune caratteristiche specifiche:

- Dominanza. L'attività domina i pensieri ed il comportamento del soggetto, assumendo un valore primario tra tutti gli interessi.
- Alterazioni del tono dell'umore. L'inizio dell'attività provoca cambiamenti nel tono dell'umore. Il soggetto prova un aumento d'eccitazione o maggiore rilassatezza come diretta conseguenza dell'incontro con l'oggetto della dipendenza.
- Conflitto. Conflitti inter-personali tra il soggetto e coloro che gli sono vicini, conflitti intrapersonali interni a se stesso, a causa del comportamento dipendente.
- Ricaduta. Tendenza a ricominciare l'attività dopo averla interrotta. I segnali patologici di questo che viene descritto come "un vero e proprio abuso della tecnologia" sono specifici così come accade per le altre dipendenze più "tradizionali". In particolare, si hanno: la tolleranza, ossia quando vi è un crescente bisogno di aumentare il tempo su internet e l'astinenza quando, cioè, vi è l'interruzione o la riduzione dell'uso della Rete che comporta ansia, agitazione psicomotoria, fantasie, pensieri ossessivi. Tutto questo ha ripercussioni sulla sfera delle relazioni interpersonali che diventano via via più povere e alle quali si preferisce il mondo virtuale, con alterazioni dell'umore e della percezione del tempo. Da sottolineare, la nomofobia (nomo deriva da "no-mobile") termine usato per categorizzare quei soggetti che sperimentano emozioni negative, quali ansia, tristezza e rabbia quando non sono connessi con il proprio smartphone. Anche qui i dati dell'Osservatorio nazionale adolescenza sembrano parlare chiaramente: "quasi 8 adolescenti su 10 hanno paura che si scarichi il cellulare o che non gli prenda quando sono fuori casa e tale condizione genera ansia, rabbia e fastidio. Spesso il trascorrere del tempo online, in termini disfunzionali, è scandito dal gioco virtuale che può anche assumere forme di Dipendenza dal gioco online (Net gaming addiction o Internet Gaming Addiction) inserito all'interno del Manuale Diagnostico Statistico dei Disturbi Mentali (DSM 5). Da specificare che la dipendenza qui si realizza quando c'è un abuso, ossia un utilizzo continuativo e sistematico della Rete al fine di giocare impegnando la maggior parte delle giornate, con la conseguente sottrazione del tempo alle altre attività quotidiane del minore.

È importante, però, non demonizzare la tecnologia o il gioco, ma azioni di formazione e/o riflessione mirate. Nel nostro Istituto scolastico si promuovono strategie per un uso più consapevole delle tecnologie per favorire il "benessere digitale", cioè la capacità di creare e mantenere una relazione sana con la tecnologia, per fare in modo che la stessa possa essere strumento per raggiungere i propri obiettivi e non solo distrazione o addirittura ostacolo.

4.5 - Sexting

Il "sexting" è fra i rischi più diffusi connessi ad un uso poco consapevole della Rete. Il termine indica un fenomeno molto frequente fra i giovanissimi che consiste nello scambio di contenuti mediali sessualmente espliciti; i/le ragazzi/e lo fanno senza essere realmente consapevoli di scambiare materiale (pedopornografico) che potrebbe arrivare in mani sbagliate e avere conseguenze impattanti emotivamente per i protagonisti delle immagini, delle foto e dei video.

Tali contenuti spesso vengono diffuse attraverso il cellulare o attraverso siti, e-mail, chat. L'invio di foto che ritraggono minorenni al di sotto dei 18 anni in pose sessualmente esplicite configura, infatti, il reato di distribuzione di materiale pedopornografico. I contenuti sessualmente espliciti, quindi, possono diventare materiale di ricatto assumendo la forma di "revenge porn" letteralmente "vendetta porno" . Si veda la Legge 19 luglio 2019 n. 69, art. 10.

Tra le caratteristiche del fenomeno vi sono principalmente:

- La fiducia tradita: chi produce e invia contenuti sessualmente espliciti ripone fiducia nel destinatario, credendo, inoltre, alla motivazione della richiesta (es. prova d'amore richiesta all'interno di una relazione sentimentale).
- La pervasività con cui si diffondono i contenuti: in pochi istanti e attraverso una condivisione che diventa virale, il contenuto a connotazione sessuale esplicita può essere diffuso a un numero esponenziale e infinito di persone e ad altrettante piattaforme differenti. Il contenuto, così, diventa facilmente modificabile, scaricabile e condivisibile e la sua trasmissione è incontrollabile.
- La persistenza del fenomeno: il materiale pubblicato online può permanervi per un tempo illimitato e potrebbe non essere mai definitivamente rimosso. Un contenuto ricevuto, infatti, può essere salvato, a sua volta re-inoltrato oppure condiviso su piattaforme diverse da quelle originarie e/o in epoche successive. A ciò si associano altri comportamenti a rischio, di tipo sessuale ma anche riferibili ad abuso di sostanze o di alcool. I rischi del sexting, legati al revenge porn, possono contemplare: violenza psicosessuale, umiliazione, bullismo, cyberbullismo, molestie, stress emotivo che si riversa anche sul corpo insieme ad ansia diffusa, sfiducia nell'altro/i e depressione.

4.6 - Adescamento online

Il ***grooming*** (dall'inglese "groom" - curare, prendersi cura) rappresenta una tecnica di manipolazione psicologica che gli adulti potenziali abusanti utilizzano per indurre i bambini/e o adolescenti a superare le resistenze emotive e instaurare una relazione intima e/o sessualizzata. Gli adulti interessati sessualmente a bambini/e e adolescenti utilizzano spesso anche gli strumenti messi a disposizione dalla Rete per entrare in contatto con loro.

I luoghi virtuali in cui si sviluppano più frequentemente tali dinamiche sono le chat, anche quelle interne ai giochi online, i social network in generale, le varie app di instant messaging (whatsapp, telegram etc.), i siti e le app di ***teen dating*** (siti di incontri per adolescenti). Un'eventuale relazione sessuale può avvenire, invece, attraverso webcam o live streaming e portare anche ad incontri dal vivo. In questi casi si parla di adescamento o grooming online.

In Italia l'adescamento si configura come reato dal 2012 (art. 609-undecies – l'adescamento di minorenni) quando è stata ratificata la Convenzione di Lanzarote (legge 172 del 1° ottobre 2012).

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere per prevenire ed affrontare la delicata problematica dell'adescamento.

A tal proposito l'Istituto ha attivato un percorso di educazione digitale che comprende lo sviluppo di capacità, quali la protezione della propria privacy e la gestione dell'immagine e dell'identità online e la capacità di gestire adeguatamente le proprie relazioni online (a partire dalla consapevolezza della peculiarità del mezzo/schermo che permette a chiunque di potersi presentare molto diversamente da come realmente è).

4.7 - Pedopornografia

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

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

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

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

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

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

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

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2023/2024).

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

☐ Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti agli/lle studenti/studentesse, con il coinvolgimento di esperti.

☐ 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/lle studenti/studentesse.

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

☐ Organizzare uno o più incontri di formazione all'utilizzo sicuro e consapevole di Internet e delle tecnologie digitali integrando lo svolgimento della didattica e assicurando la partecipazione attiva degli studenti/studentesse.

☐ Promuovere incontri e laboratori per studenti e studentesse dedicati all' Educazione Civica Digitale.

☐ Organizzare uno o più incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/lle studenti/studentesse.

☐ Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/lle 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 minorenne e inoltre è importante non sostituirsi al bambino/a e/o adolescente, evitando, quindi, di rispondere all'adescatore al suo posto). È fondamentale valutare il benessere psicofisico dei minori e il rischio che corrono. Vi ricordiamo che l'attuale normativa prevede che la persona coinvolta in qualità di vittima o testimone in alcune tipologie di reati, tra cui il grooming, debba essere ascoltata in sede di raccolta di informazioni con l'ausilio di una persona esperta in psicologia o psichiatria infantile.
- **Sexting**: nel caso in cui immagini e/o video, anche prodotte autonomamente da persone minorenni, sfuggano al loro controllo e vengano diffuse senza il loro consenso è opportuno adottare sistemi di segnalazione con l'obiettivo primario di tutelare il minore e ottenere la rimozione del materiale, per quanto possibile, se online e il blocco della sua diffusione via dispositivi mobili.

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

Vi suggeriamo, inoltre, i seguenti servizi:

- Servizio di Helpline 19696 e Chat di Telefono Azzurro per supporto ed emergenze;

- Clicca e segnala di Telefono Azzurro e STOP-IT di Save the Children Italia per

segnalare la presenza di materiale pedopornografico online.

5.2. - Come segnalare: quali strumenti e a chi

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

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

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

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

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

Strumenti a disposizione di studenti/esse

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

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

Anche studenti e studentesse, inoltre, possono rivolgersi alla Helpline del progetto

Generazioni Connesse, al numero gratuito 1.96.96.

Segnalare un atto di bullismo all'interno della scuola rappresenta uno dei passaggi chiave del processo di prevenzione di questo fenomeno. Proprio per tale motivo l'Istituto ha ritenuto indispensabile, nonchè doveroso, creare uno spazio virtuale attraverso il quale i docenti, il personale ATA, i genitori e gli allievi possono denunciare eventuali casi di bullismo in totale riservatezza.

L'Istituto Tecnico Industriale "A. Monaco" al fine di aiutare gli studenti a segnalare eventuali situazioni problematiche, ha previsto i seguenti strumenti:

1. un indirizzo e-mail specifico per le segnalazioni: **bullismo@itimonaco.it**.
2. il modulo di segnalazione dei casi.
3. lo sportello di ascolto gestito da professionisti.
4. il docente Referente ed il Team bullismo e cyberbullismo.

La segnalazione del caso dovrà essere avviata attraverso il modulo allegato al presente documento (All.1) e presa in carico dalla Referente, la quale, insieme al Team si occuperà di raccogliere tutte le informazioni e di segnalare l'evento al Dirigente Scolastico, che valuterà, insieme al gruppo specializzato, se il caso vada gestito all'interno della scuola o attraverso il coinvolgimento di organi di stato competenti.

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.

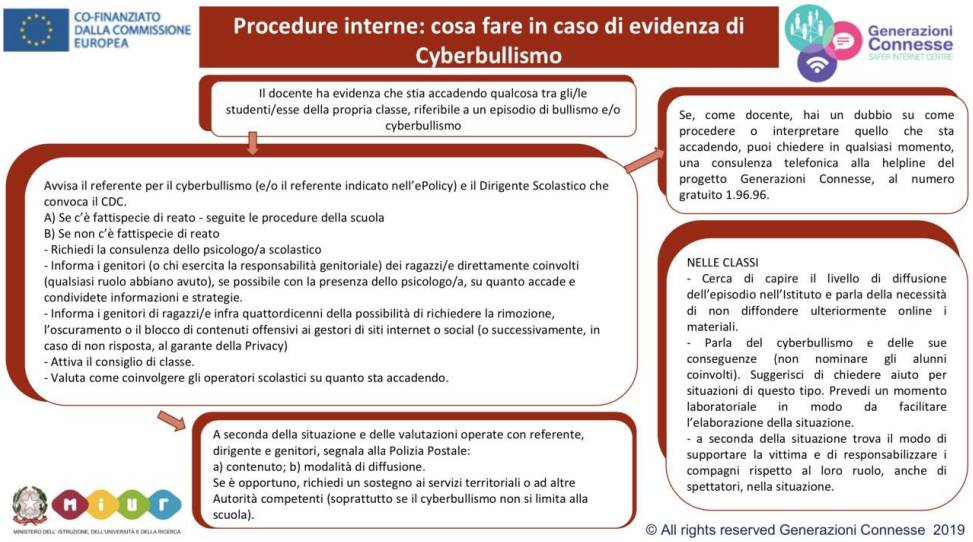
A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all'utilizzo di Internet può presentare.

- **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.

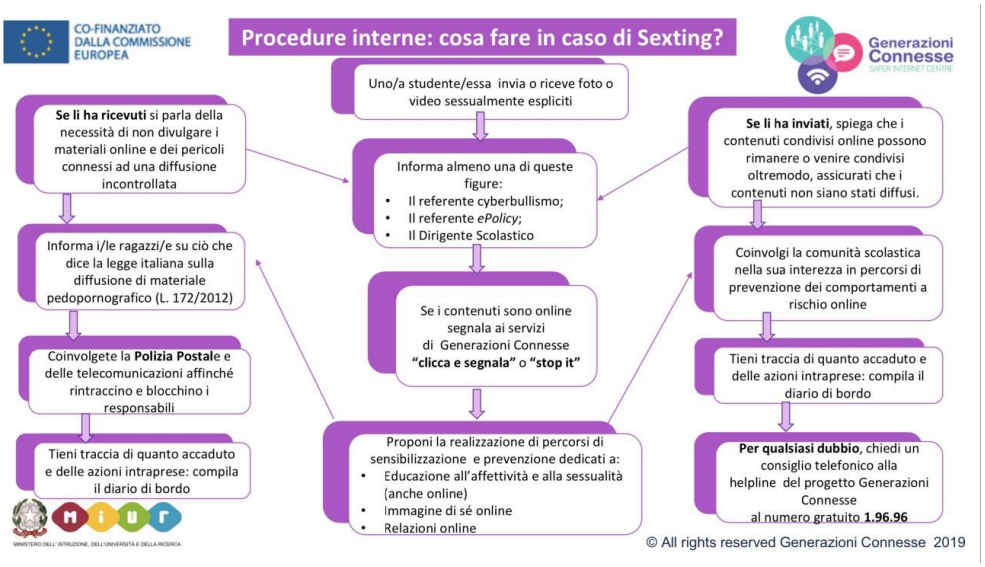
L'Istituto Tecnico Industriale "A. Monaco" ha evidenziato all'interno del Vademecum "Bullismo e Cyberbullismo" allegato al PTOF 2019-2022, le agenzie territoriali deputate alla presa in carico di tali problematiche.

5.4. - Allegati con le procedure

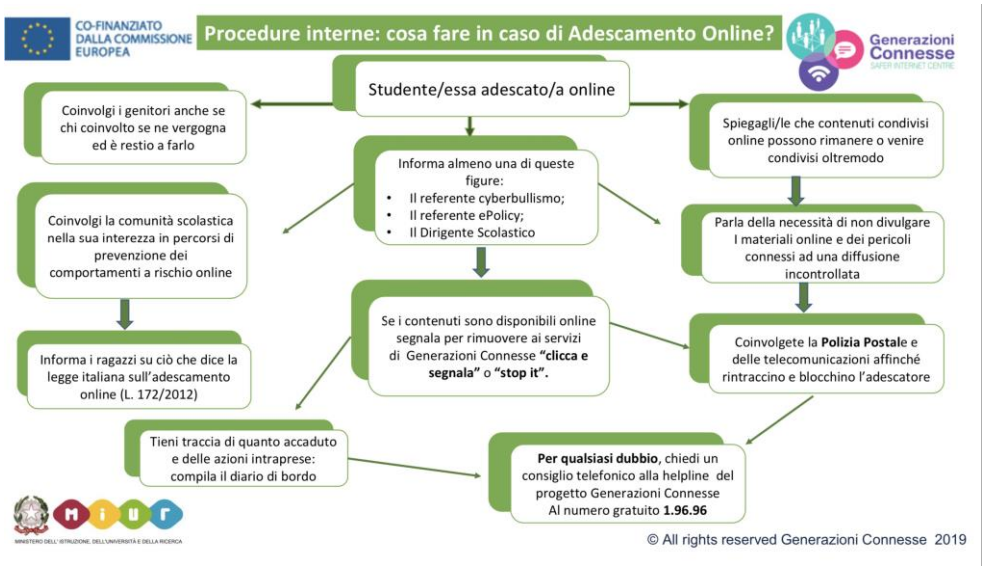
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



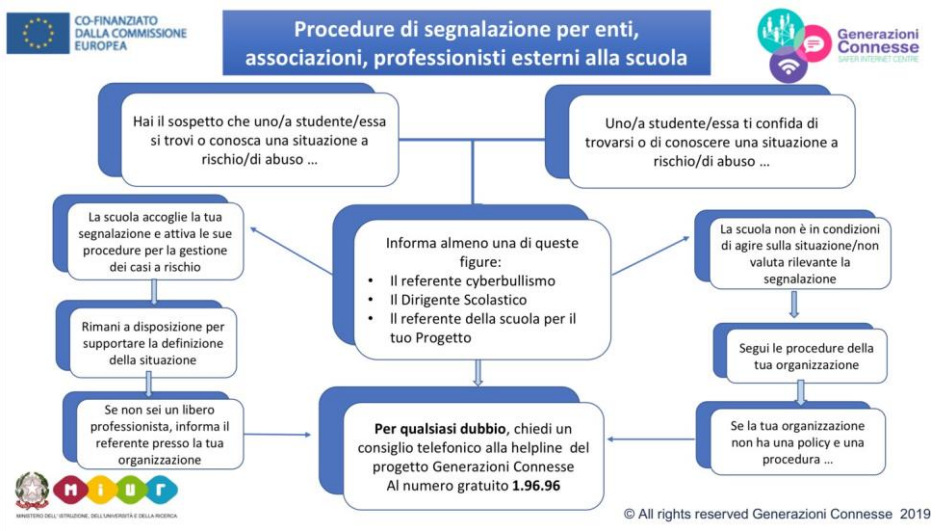
Procedure interne: cosa fare in caso di sexting?



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

Allegato 1

ISTITUTO TECNICO INDUSTRIALE "A. MONACO"

MODELLO PER SEGNALARE EPISODI DI BULLISMO E CYBERBULLISMO A SCUOLA

DATA____/____/_____

Nome e cognome di chi effettua la segnalazione: _____

Nome e cognome di chi ha subito atti di bullismo/cyberbullismo: _____Classe_____

Nome e cognome di chi ha compiuto atti di bullismo/cyberbullismo: _____Classe_____

1. La segnalazione del presunto caso di bullismo è stata fatta (indicare il nome):

- Dalla

VITTIMA_____

_

- Da un compagno della vittima _____
- Dalla madre/dal padre /dal tutore della vittima _____
- Da un insegnante _____

2. Gli episodi sono stati segnalati anche da altre persone (indicare il nome)?
   - Da un compagno della vittima _____
   - Dalla madre/dal padre /dal tutore della vittima _____
   - Da un insegnante _____
3. Tipologia dell'episodio
   - Bullismo
   - Cyberbullismo
4. Breve descrizione del problema presentato. Fare esempi concreti degli episodi di prepotenza (dove e quando?)
   _____
   _____
   _____
   _____
   _
5. Quante volte si sono verificati gli episodi?
   _____
   _____
   _____
   _____
   _

FIRMA

_____

Allegato 2

DICHIARAZIONE LIBERATORIA PER FOTOGRAFIE E RIPRESE VIDEO

(D.Lgs. 196/2003 "Codice in materia di protezione dei dati personali" - Regolamento Europeo sulla privacy GDPR 2016/679).

Il sottoscritto_____, nato a_____(_____), il__/ ___/ _____, residente in _____ (____), indirizzo: _____;

La sottoscritta_____, nata a_____(_____), il___/_____/ ______, residente in _____ (____), indirizzo: _____.

Genitori dell'alunno/a_____iscritto/a alla classe____per l'A.S._____

A U T O R I Z Z A N O

L'Istituzione scolastica, nella persona del Dirigente Scolastico, a poter effettuare ed utilizzare fotografie, video o altri materiali audiovisivi contenenti l'immagine, il nome e la voce del proprio figlio/a, all'interno di attività educative e didattiche e/o dichiarazioni e commenti personali registrati all'interno delle attività curriculari ed extracurriculari programmate nel PTOF dell'Istituto, per scopi documentativi, formativi e informativi.

Il Dirigente Scolastico assicura che le immagini e le riprese audio-video realizzate dalla scuola, nonché gli elaborati prodotti dagli studenti durante le attività scolastiche, potranno essere utilizzati esclusivamente per documentare e divulgare le attività della scuola tramite il sito internet di Istituto, pubblicazioni, mostre, corsi di formazione, seminari, convegni e altre iniziative promosse dall'Istituto anche in collaborazione con altri enti pubblici, sempre nell'ambito della formazione.

La presente autorizzazione non consente l'uso dell'immagine in contesti che pregiudichino la dignità personale ed il decoro del minore e comunque per uso e/o fini diversi da quelli sopra indicati ed è valida fino al compimento della maggiore età dell'alunno/a. In qualsiasi momento sarà possibile revocare il consenso al trattamento specifico e richiedere la rimozione di dati e fotografie riguardanti il minore, (art.17 del GDPR) inviando una e-mail all'indirizzo mail istituzionale. Tale revoca non preclude la liceità del trattamento effettuato in base al consenso prestato anteriormente alla revoca.

La presente autorizzazione è da ritenersi valida per tutto il corso di studi dell'alunna/o presso l'Istituto.

Luogo e data _____

In fede

_____ _____

_____

(firma del D.S.) (firma dei genitori)

Il nostro piano d'azioni

Mediante interventi specifici l'Istituto "A. Monaco" intende promuovere, entro le classi, un clima collaborativo orientato a far emergere e a riconoscere quanto prima un problema di bullismo e cyberbullismo per innescare un processo di cambiamento nelle dinamiche del gruppo classe.

Nel caso invece in cui vi siano segnalazioni o sospetti di bullismo, si procede all'ascolto degli alunni coinvolti con l'obiettivo di acquisire informazioni aggiuntive, cercando di creare delle situazioni di dialogo tra gli alunni stessi, volte a far emergere i fatti. Qualora i fatti venissero accertati, l'Istituto si avvale del proprio regolamento al fine di attivare tutte le procedure previste.