Istituto Omnicomprensivo
"Salvatorelli-Moneta"
Marsciano

Documento di ePolicy

PGIS00300E

I.O. "SALVATORELLI-MONETA"

VIA CARDINALE FRANCESCO SATOLLI 4 - 06055 - MARSCIANO - PERUGIA (PG)

Mariangela Severi

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.

Il presente Documento E-Policy viene redatto dall'I.O Salvatorelli Moneta di Marsciano nell'Anno Scolastico 2022/2023 ed è parte integrante del Piano Triennale dell'Offerta Formativa.

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 con le tecnologie digitali, oltre che di sensibilizzazione su un uso consapevole delle stesse.

Finalità del presente documento è regolamentare in modo organico e condiviso dall'intera Comunità Scolastica i comportamenti e le procedure in merito all'utilizzo delle Tecnologie dell'Informazione e della Comunicazione (TIC) nella didattica, promuoverne un uso critico e consapevole, prevenire, rilevare, gestire e contrastare le problematiche derivanti da un uso ignaro ed improprio delle tecnologie digitali. Il Piano Nazionale Scuola Digitale affida esplicitamente alla scuola il compito di rafforzare le competenze digitali per consentire ai cittadini di domani di esercitare pienamente i loro diritti e di abitare in maniera consapevole il mondo sempre più "glocale". Il nostro Istituto riconosce come le TIC rappresentino una grande opportunità per sostenere l'insegnamento, promuovere la creatività, stimolare la consapevolezza e migliorare l'apprendimento degli studenti, ma è conscio dei rischi relativi e della conseguente necessità di fronteggiarli adeguatamente.

Il nostro Istituto, con questa E-policy, ha deciso di adottare una politica di prevenzione attraverso:

- La messa in campo di azioni informative e di confronto volte al riconoscimento precoce di comportamenti a rischio con lo scopo di intervenire prima della possibile insorgenza di fenomeni veri e propri di bullismo e /o cyberbullismo, azioni che possano promuovere l'uso consapevole e funzionale delle tecnologie e dei social.
- La promozione di interventi educativi e azioni a supporto di studenti e studentesse vittime di cyberbullismo o di problematiche relative all'utilizzo della rete, in linea con la legge 71/2017 "Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo".

- La realizzazione di progetti d'Istituto che siano caratterizzati da multidisciplinarietà con il coinvolgimento e il supporto di figure esterne qualificate (es. educatori, psicologi, esperti informatici, polizia postale, ecc.).
- La sottoscrizione di un codice di condotta e di un'autocertificazione ai sensi dell'art.2 del D. Lgs. n.39/2014, da parte di tutti coloro (dipendenti, collaboratori, esperti, volontari) che abbiano contatti diretti con i minori.

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.

Ogni utente appartenente alla comunità educante nel momento in cui utilizza la rete deve:

- rispettare il presente documento e la normativa vigente;
- tutelare la privacy di tutti gli utenti coinvolti;
- rispettare la "netiquette", galateo della rete.

All'interno della comunità educante ogni figura ha un ruolo specifico:

- I**l Dirigente Scolastico** promuove l'uso consapevole delle tecnologie e di internet garantendo la sicurezza, anche online, di tutti i membri della comunità scolastica, in linea con il quadro normativo di riferimento e le indicazioni del MIUR; inoltre ha il compito di promuovere la sicurezza online dando il proprio contributo all'organizzazione, insieme al TIM prevenzione bullismo/cyberbullismo, di corsi di formazione specifici per tutte le figure scolastiche, sull' utilizzo positivo e responsabile delle TIC. In caso di episodi manifesti di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali ha il compito di intervenire sia sul piano educativo che sanzionatori.
- **DS con DSGA (GESTORI DATI E INFORMAZIONI)**
  Assicurare nei limiti delle risorse finanziarie disponibili l'intervento di tecnici per garantire che l'infrastruttura tecnologica della scuola sia funzionante, sicura, non aperta ad uso improprio o a dannosi attacchi esterni;
  Favorire il funzionamento dei diversi canali di comunicazione all'interno della scuola e fra la scuola e le famiglie;
  Garantire che i dati di gestione siano accurati e aggiornati;
  Promuovere le migliori pratiche nella gestione delle informazioni, ossia mettere in atto un sistema di controllo di accesso appropriato. I dati sono utilizzati, trasferiti e cancellati in linea con i requisiti di protezione dei dati;
  Mantenere i controlli di accesso per proteggere le informazioni sensibili

archiviati su
dispositivi di proprietà della scuola.

- **L'Animatore digitale** ha il compito di promuovere corsi di formazione d'Istituto sulle TIC, supportare il personale scolastico sia dal punto di vista tecnico e informatico sia in merito alla tutela della privacy e inoltre può monitorare e rilevare eventuali episodi o problematiche connesse all'uso delle TIC a scuola controllando che tutti 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"), ha il compito di coordinare e promuovere azioni specifiche per la prevenzione e il contrasto del fenomeno del bullismo e del cyberbullismo. La scuola può avvalersi della collaborazione delle Istituzioni, delle Forze di polizia, delle associazioni e dei centri di aggregazione giovanile del territorio. Il team prevenzione bullismo e cyberbullismo può coinvolgere in progetti e percorsi formativi tutta la comunità educante.
- **I Docenti** hanno un ruolo molto importante poiché hanno il compito di diffondere la cultura dell'uso responsabile e consapevole delle TIC e della Rete. Possono utilizzare le TIC nella didattica della propria disciplina per offrire ai ragazzi più strumenti mettendo così tutti i ragazzi nelle condizioni di poterli utilizzare senza mettere in "risalto" gli alunni con BES. I docenti devono supportare gli studenti nelle attività di apprendimento e nei laboratori che prevedono l'uso della LIM o di altri dispositivi tecnologici connessi in Rete. Inoltre hanno il compito di educare gli studenti all'importanza del rispetto della privacy ricordando loro di segnalare sempre eventuali siti che possono spaventare o comunicare ai genitori di aver conosciuto persone online. E' importante che gli alunni siano informati sui rischi presenti in Rete, vanno educati ad un uso consapevole in modo che Internet possa essere per i ragazzi una fonte di divertimento oltre che un utile strumento di apprendimento. I docenti devono osservare i comportamenti a rischio dei ragazzi e hanno il dovere morale e professionale di segnalare al Dirigente Scolastico che insieme al Referente per il Cyberbullismo e al Consiglio di Classe potrà definire strategie di intervento condivise.
- **Personale ATA** Esiste un concreto coinvolgimento del personale ATA nell'applicazione della legge 107/15 ("La Buona Scuola") che concerne non solo il tempo scuola e il potenziamento dell'offerta formativa, ma anche le attività di formazione e autoformazione in tema di bullismo e cyberbullismo. Il personale ATA è coinvolto nelle pratiche di prevenzione perchè è tenuto alla segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo.
- **Gli Studenti e le Studentesse** devono di mostrare di saper utilizzare in modo consapevole le tecnologie digitali in coerenza con quanto richiesto dai docenti.

Con il supporto della scuola devono partecipare ai progetti e alle attività proposte sull'utilizzo consapevole delle TIC dovrebbero imparare a tutelarsi online, potrebbero inoltre promuovere percorsi di peer education per aiutare i compagni più piccoli in questo percorso di crescita favorendo una continuità verticale che è molto a cuore al nostro Istituto.

- **I Genitori** hanno il compito di collaborare con l'Istituto scolastico, sono attori partecipi e attivi nelle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete, nonché sull'uso responsabile dei device personali. Come parte della comunità educante sono tenuti a relazionarsi con i docenti sulle linee educative che riguardano le TIC e la Rete e hanno il dovere di confrontarsi con loro nel momento in cui rilevano che i propri figli fanno un uso scorretto e poco responsabile delle tecnologie digitali o di Internet. È importante che accettino e condividano quanto scritto nell'ePolicy dell'Istituto e nel patto di responsabilità in un'ottica di collaborazione reciproca. Bisogna, inoltre, ricordare 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 (...)".

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).

Gli Enti educativi esterni e le Associazioni che entrano in relazione con la scuola devono conformarsi alla politica della stessa riguardo all'uso consapevole della Rete e delle TIC; devono, inoltre, promuovere comportamenti sicuri, la sicurezza online e assicurare la protezione degli studenti e delle studentesse durante le attività che si svolgono insieme.

Nella realizzazione di progetti, le collaborazioni con enti o figure esterne devono essere preventivamente concordate con il TEAM prevenzione bullismo e cyberbullismo e autorizzate dal Dirigente scolastico.

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.

Il documento E-Safety Policy verrà pubblicato sul sito della scuola e condiviso con tutta la comunità educante. Tutti gli alunni saranno informati che la rete, l'uso di Internet e di ogni dispositivo digitale saranno utilizzati solo con l'autorizzazione degli insegnanti. Gli alunni verranno educati all'uso responsabile e sicuro di internet prima che venga permesso loro l'accesso alla rete a scuola. L'elenco delle regole per la sicurezza on-line sarà pubblicato in tutte le aule o laboratori con accesso a internet.

Il documento sarà discusso e condiviso negli organi collegiali e successivamente sarà condiviso con i genitori all'interno dei singoli consigli di classe. Per il nuovo personale e i nuovi alunni: la e-policy sarà consegnata insieme agli altri documenti da sottoscrivere all'atto della stipula del contratto/iscrizione. Per tutto il personale sono previsti aggiornamenti e nuova formazione in materia di sicurezza online.

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 sanzioni, riferite soprattutto agli alunni, avranno come carattere preferenziale quello educativo/riabilitativo e in ogni caso verrà coinvolta la componente genitori, in qualità di primi educatori.
Le infrazioni saranno riferite direttamente al Dirigente Scolastico.
La scuola adotterà tutte le misure necessarie per garantire agli studenti l'accesso a materiale e ambienti appropriati, anche se è impossibile evitare in assoluto che essi trovino materiale indesiderato navigando in rete a scuola. La scuola non può farsi carico della responsabilità per il materiale trovato su internet o per eventuali conseguenze causate dall'accesso ad internet. Qualsiasi sospetto, rischio, uso improprio, violazione vanno segnalati immediatamente al Dirigente che, eventualmente, riferisce direttamente alle autorità di competenza (v. protocollo dei rischi rilevati). Al personale, agli studenti e agli altri componenti della comunità scolastica sono date informazioni sulle infrazioni previste le eventuali sanzioni.

1.6 - Integrazione dell'ePolicy con Regolamenti esistenti

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

Il presente documento si armonizza con gli obiettivi e i contenuti del PTOF e del Regolamento d'Istituto. Integra tali regolamenti costituendo la sezione relativa all'uso delle nuove tecnologie, dei nuovi ambienti di apprendimento e delle metodologie didattiche offerti dall'Istituto (scuola 2.0, etc.). La commissione E-policy opera al fine di integrare i regolamenti dell'Istituto con il presente documento, apportandone le opportune modifiche da proporre al Collegio Docenti.

1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

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

Il monitoraggio e l'aggiornamento annuali sarannò affidati alla commissione E-policy e supervisionata dal Dirigente Scolastico.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

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

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

Azioni da svolgere nei prossimi 3 anni:

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

Capitolo 2 - Formazione e 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.

La competenza digitale, per la sua importanza nelle attività professionali e anche quotidiane, è ritenuta dall'Unione Europea una competenza chiave per lo sviluppo del senso di cittadinanza. Nel curricolo disciplinare del nostro Istituto tale competenza pervade in modo trasversale i vari insegnamenti; questa declinazione scaturisce dalla necessità di iniziare a dare una formazione di base sull'uso delle TIC, inserendole nelle attività didattiche, per arrivare nelle classi finali a fornire gli strumenti per un approccio consapevole, critico, autonomo e responsabile. Tali competenze sono oggetto di certificazione, come da apposito documento ministeriale, al termine della scuola Primaria e Secondaria. Negli ultimi anni la scuola ha provveduto all'implementazione della dotazione digitale dei vari plessi, anche attraverso la partecipazione ai progetti PON, per
consentire l'introduzione di metodologie basate sull'uso delle TIC.

Il nostrio istituto, al fine della creazione di competenze digitali per gli studenti,

personalizzate e orientanti rispetto al contesto territoriale e internazionale nel quale si trovano comunque a crescere operando scelte consapevoli, ha creato una serie di iniziative volte a sviluppare competenze in ambito tecnologico e sociale. Esempi significativi in tal senso sono i progetti di seguito elencati:

* "Un patentino per lo Smartphone", attivato per la SS1, prevede finalizzato all'uso consapevole dello smartphone, all'acquisizione di comportamenti corretti e funzionali nel navigare, nell'essere fruitori e protagonisti attivi nella circolazione delle informazioni e nella relazione online.

* Incontri con la Polizia postale, attivato per la SS2, per la sensibilizzazione ai rischi e alle complessità che la rete nasconde e quindi per maturare in ogni studente una maggiore competenza nell'ambito della cybersicurezza.

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.

I docenti, in conformità con quanto previsto dal piano triennale dell'offerta formativa, hanno partecipato a corsi di formazione nell'ambito di piani nazionali e ad iniziative organizzate dall'istituzione o dalle scuole associate in rete incrementando le competenze digitali di base. I docenti del team digitale stanno seguendo la formazione ad essi destinata, che si auspica sia spendibile all'interno dell'Istituto. Nel corso del corrente anno il team digitale intende promuovere iniziative di autoformazione interna gestita da docenti dell'istituto; inoltre i docenti potranno avvalersi dei corsi di aggiornamento promossi dall'Ambito Territoriale TO07 oppure presenti sulla piattaforma SOFIA riguardanti l'innovazione didattica e la didattica digitale.

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.

La formazione specifica dei docenti sull'utilizzo consapevole e sicuro di Internet può prevedere momenti di autoaggiornamento, momenti di formazione personale o collettiva di carattere permanente, legata all'evoluzione rapida delle tecnologie e delle modalità di comunicazione a cui accedono sempre di più ed autonomamente anche i ragazzi.

In merito al piano di azioni di prevenzione e contrasto ai fenomeni di bullismo e cyberbullismo condivise dal Gruppo di lavoro integrato dell'USR Umbria, conclusa la prima fase rivolta agli studenti, l'USR ha organizzato degli incontri formativi rivolti ai docenti a cura di "PEPITA ONLUS". La formazione prevede due incontri in presenza: in uno verrà affrontato l'aspetto psicologico- educativo, con particolare attenzione alle numerose applicazioni utilizzate dai giovani e giovanissimi che nascondono insidie sempre più complesse e difficili da individuare ma che d'altro canto li attraggono in età sempre più precoce; l'altro incontro riguarderà l'aspetto legale, la tutela dei ragazzi ma anche del personale scolastico e della responsabilità dei genitori.

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.

L'Istituto ha promosso e continua a promuovere iniziative per sensibilizzare le famiglie all'uso consapevole delle TIC e della rete, promuovendo la conoscenza delle numerose situazioni di rischio online. A tal fine sono previsti incontri fra genitori e specialisti (docenti, forze dell'ordine) per la diffusione del materiale informativo su queste tematiche. Saranno favoriti momenti di confronto e discussione anche sulle dinamiche che potrebbero instaurarsi fra i pari con l'uso di cellulari e smartphone o delle chat line o social network più diffusi, con particolare riferimento alla prevenzione del cyberbullismo. Sul sito scolastico e sulla relativa bacheca virtuale relativa a "Generazioni connesse" saranno messi in condivisione materiali dedicati ad alunni e alle famiglie come guide in formato pdf e video che possono fornire spunti di approfondimento e confronto. La scuola si impegna alla diffusione delle informazioni e delle procedure contenute nel documento (Policy e-safety) per portare a conoscenza delle famiglie il regolamento sull'utilizzo delle nuove tecnologie all'interno dell'istituto e prevenire i rischi legati a un utilizzo non corretto di internet. L'istituto intrattiene rapporti costanti e sistematici con le famiglie e li informa, tramite il registro elettronico, delle attività proposte a genitori e studenti. Comunica l'andamento didattico-disciplinare dei singoli alunni tramite il coordinatore di classe e/o il responsabile di plesso, nonché il singolo insegnante. In questo senso, la Scuola ha elaborato il Patto Educativo di Corresponsabilità che rappresenta un'alleanza educativa ove sono definiti in maniera dettagliata e condivisa i diritti e i doveri presenti nel rapporto tra Istituzione scolastica autonoma, studenti e famiglie. Con la sottoscrizione del Patto Educativo i firmatari si assumono precise responsabilità anche in conformità con la normativa vigente.

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.

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

- Organizzare incontri con esperti per i docenti sulle competenze 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.

Il trattamento dei dati personali, ai sensi e per l'effetto della legge 31/12/1996 n. 675 e del GDPR Regolamento UE 2016/679, è informato ai principi del rispetto dei diritti, delle libertà fondamentali e della dignità delle persone con particolare riferimento alla riservatezza e all'identità personale. L'impegno sarà rivolto a non diffondere i dati personali in possesso della scuola, siano essi relativi agli studenti che al personale, ad enti esterni se non per gli obblighi di legge. Diritto alla riservatezza per gli studenti maggiorenni (D. Lgs. 196/2003)

A - Gli studenti maggiorenni, nonché gli studenti che raggiungeranno la maggiore età nel corso dell'anno scolastico, entro la data prevista per l'inizio dei colloqui scuola-famiglia presentano al docente Coordinatore di classe una dichiarazione, con la quale autorizzano o meno i Docenti del Consiglio di Classe a comunicare ai genitori, o a chi ne fa le veci, ogni informazione relativa al proprio andamento scolastico.

B - La scelta effettuata ha validità per l'anno scolastico in Corso, ma può in ogni momento essere modificata dall'interessato, presentando al Coordinatore di classe un'ulteriore dichiarazione correttiva.

C - Il docente Coordinatore, ricevute le dichiarazioni in parola, che saranno conservate agli atti dell'Ufficio di Segreteria dell'Istituto, dà tempestiva comunicazione a tutti i Docenti del Consiglio di classe dei nominativi degli studenti che non hanno autorizzato la comunicazione con le famiglie. In difetto di autorizzazione, i Docenti hanno l'obbligo di astenersi dal comunicare qualsiasi informazione relativa allo studente.

D - Gli studenti maggiorenni che intendono avvalersi del diritto alla riservatezza sono sollevati dall'obbligo di trasmettere alla famiglia le comunicazioni della scuola.

E -L'Istituto comunicherà alla famiglia la richiesta dello studente di avvalersi del diritto alla riservatezza entro 15 giorni dall'istanza.

Tutto il personale è inoltre tenuto al segreto d'ufficio, ossia non può dare informazioni o comunicazioni relative ad operazioni amministrative di qualsiasi natura o notizie relative a fatti e persone delle quali sia venuto a conoscenza in occasione e/o durante il servizio.

Gli insegnanti dell'Istituto sono nominati dal Dirigente scolastico quali incaricati del trattamento dei dati personali degli alunni e delle loro famiglie ai fini dello svolgimento delle proprie funzioni istituzionali e nel rispetto della normativa vigente.

I genitori degli alunni o chi riveste la responsabilità genitoriale:

a) prendono visione dell'Informativa sulla privacy dell'Istituto ai sensi dell'art. 13 del Regolamento UE 2016/679 (GDPR);

b) prendono visione dell'Informativa per il trattamento dei dati personali ai fini dell'utilizzo della piattaforma "Google Workspace for Education Fundamentals" (per maggiorenni e per minorenni) ai sensi dell'art. 13 del Reg. UE 2016/679 - GDPR sull'utilizzo della Google Workspace for Education Fundamentals, comprendente anche la Netiquette ovvero dell'insieme di regole che disciplinano il comportamento delle studentesse e degli studenti in rapporto all'utilizzo degli strumenti digitali;

c) sottoscrivono il Patto educativo di corresponsabilità

AUTORIZZAZIONE ALLA RIPRESA E ALL'USO DI IMMAGINI E REGISTRAZIONI SONORE E ALLA DIVULGAZIONE DI ELABORATI PRODOTTI DAGLI STUDENTI

Preso atto dell'Informativa fornita ai sensi dell'art. 13 del Reg. UE 2016/679 - GDPR dall'Istituto in via Cardinale Francesco Satolli, 4 - 06055 - Marsciano - Codice meccanografico PGIS00300E io sottoscritto/a nome _____ cognome _____ nato/a a _____ il _____, frequentante la classe _____ relativamente alle seguenti attività:

1. realizzazione di fotografie, video o altri materiali audiovisivi contenenti gli elaborati prodotti durante le attività didattiche e formative, la mia immagine, il mio nominativo e la mia voce all'interno di attività educative e didattiche scolastiche o extrascolastiche

□ ESPRIMO IL MIO CONSENSO □ NEGO IL MIO CONSENSO

2. utilizzo, comunicazione a soggetti individuati dall'Istituto scolastico (es. famiglie degli allievi della Scuola, altri Istituti scolastici, Enti, ecc.) e diffusione degli elaborati prodotti durante le attività didattiche e formative, del mio nominativo, della mia voce e della mia immagine fotografata/registrata durante le attività sopra descritte e nell'ambito delle finalità istituzionali della Scuola, attraverso affissioni interne ed esterne alla scuola, attraverso il sito web dell'Istituto e le pagine ufficiali dello stesso sui social media (es. Facebook, Instagram, YouTube), attraverso gli organi di stampa ed i media televisivi ed attraverso ogni altro canale o modalità di comunicazione, senza scopo di lucro, a fini documentativi, formativi e informativi sulla vita della Scuola e delle attività scolastiche o extrascolastiche, la conservazione nell'archivio storico della Scuola e il possibile trasferimento dei dati in Paesi non facenti parte dell'Unione Europea come descritto nell'Informativa

□ ESPRIMO IL MIO CONSENSO □ NEGO IL MIO CONSENSO

3. trasferimento degli elaborati prodotti durante le attività didattiche e formative, del mio nominativo e della mia immagine ad editori o soggetti curatori di volumi inerenti

le attività e le finalità della Scuola, che potranno anche porre in vendita le opere pubblicate, fermo restando la titolarità del materiale in capo all'Istituto scolastico, e il possibile trasferimento dei predetti dati in Paesi non facenti parte dell'Unione Europea come descritto nell'Informativa

☐ESPRIMO IL MIO CONSENSO ☐NEGO IL MIO CONSENSO

4. trasferimento degli elaborati prodotti durante le attività didattiche e formative, del mio nominativo, della mia immagine e della registrazione audio della mia voce a soggetti promotori e/o organizzatori di concorsi, progetti, manifestazioni ed eventi per la partecipazione degli studenti o dell'Istituto scolastico agli stessi e il possibile trasferimento dei dati in Paesi non facenti parte dell'Unione Europea come descritto nell'Informativa

☐ESPRIMO IL MIO CONSENSO ☐NEGO IL MIO CONSENSO

5. utilizzo e pubblicazione degli elaborati prodotti durante le attività didattiche e formative, del mio nominativo, della mia voce e delle mia immagini per la presentazione e la promozione dell'offerta formativa e delle attività dell'Istituto Scolastico, in occasione dell'Open Day e in ogni altra circostanza in cui sia necessaria o in cui l'Istituto scolastico ritenga opportuna una presentazione e/o una promozione dell'Istituto scolastico (es. iscrizione nuovo anno scolastico, partecipazione a concorsi, eventi, riconoscimenti), attraverso le visite virtuali dell'Istituto scolastico, le videoconferenze, la comunicazione del materiale a soggetti individuati dall'Istituto scolastico, la pubblicazione sul sito web dell'Istituto e le pagine ufficiali dello stesso sui social media (es. Facebook, Instagram, YouTube), oppure attraverso gli organi di stampa, i media televisivi e ogni altro canale o modalità di comunicazione e il possibile trasferimento dei dati in Paesi non facenti parte dell'Unione come descritto nell'Informativa

☐ ESPRIMO IL MIO CONSENSO ☐ NEGO IL MIO CONSENSO

Nel caso di consenso, DICHIARO anche in riferimento agli artt. 9 e 10 del Codice civile (diritto al nome e all'immagine) e degli artt. 96 e 97 della Legge n. 633/1941 - Legge sul diritto d'autore (diritti relativi al ritratto), di non aver nulla a pretendere, nei confronti della Scuola, in ragione di quanto sopra indicato e di rinunciare irrevocabilmente ad ogni diritto, azione o pretesa derivante da quanto sopra autorizzato. Rimangono salvi i diritti dell'Interessato previsti dal Reg. UE 2016/679 - GDPR (artt. 7 e 15 e seguenti) come indicato nell'Informativa.

Data _____ Firma _____

AUTORIZZAZIONE ALLA RIPRESA E ALL'USO DI IMMAGINI E REGISTRAZIONI SONORE E ALLA DIVULGAZIONE DI ELABORATI PRODOTTI DAGLI STUDENTI (MINORENNI)

Preso atto dell'Informativa fornita ai sensi dell'art. 13 del Reg. UE 2016/679 - GDPR dall'Istituto in via Cardinale Francesco Satolli, 4 - 06055 - Marsciano - Codice meccanografico PGIS00300E io sottoscritto/a nome _____ cognome _____ nato/a a _____ il _____, frequentante la classe _____ relativamente alle seguenti attività:

1. realizzazione di fotografie, video o altri materiali audiovisivi contenenti gli elaborati prodotti durante le attività didattiche e formative, la mia immagine, il mio nominativo e la mia voce all'interno di attività educative e didattiche scolastiche o extrascolastiche

□ ESPRIMO IL MIO CONSENSO □ NEGO IL MIO CONSENSO

2. utilizzo, comunicazione a soggetti individuati dall'Istituto scolastico (es. famiglie degli allievi della Scuola, altri Istituti scolastici, Enti, ecc.) e diffusione degli elaborati prodotti durante le attività didattiche e formative, del mio nominativo, della mia voce e della mia immagine fotografata/registrata durante le attività sopra descritte e nell'ambito delle finalità istituzionali della Scuola, attraverso affissioni interne ed esterne alla scuola, attraverso il sito web dell'Istituto e le pagine ufficiali dello stesso sui social media (es. Facebook, Instagram, YouTube), attraverso gli organi di stampa ed i media televisivi ed attraverso ogni altro canale o modalità di comunicazione, senza scopo di lucro, a fini documentativi, formativi e informativi sulla vita della Scuola e delle attività scolastiche o extrascolastiche, la conservazione nell'archivio storico della Scuola e il possibile trasferimento dei dati in Paesi non facenti parte dell'Unione Europea come descritto nell'Informativa

□ ESPRIMO IL MIO CONSENSO □ NEGO IL MIO CONSENSO

3. trasferimento degli elaborati prodotti durante le attività didattiche e formative, del mio nominativo e della mia immagine ad editori o soggetti curatori di volumi inerenti le attività e le finalità della Scuola, che potranno anche porre in vendita le opere pubblicate, fermo restando la titolarità del materiale in capo all'Istituto scolastico, e il possibile trasferimento dei predetti dati in Paesi non facenti parte dell'Unione Europea come descritto nell'Informativa

□ESPRIMO IL MIO CONSENSO □NEGO IL MIO CONSENSO

4. trasferimento degli elaborati prodotti durante le attività didattiche e formative, del mio nominativo, della mia immagine e della registrazione audio della mia voce a soggetti promotori e/o organizzatori di concorsi, progetti, manifestazioni ed eventi per la partecipazione degli studenti o dell'Istituto scolastico agli stessi e il possibile trasferimento dei dati in Paesi non facenti parte dell'Unione Europea come descritto

nell'Informativa

□ESPRIMO IL MIO CONSENSO □NEGO IL MIO CONSENSO

5. utilizzo e pubblicazione degli elaborati prodotti durante le attività didattiche e formative, del mio nominativo, della mia voce e delle mia immagini per la presentazione e la promozione dell'offerta formativa e delle attività dell'Istituto Scolastico, in occasione dell'Open Day e in ogni altra circostanza in cui sia necessaria o in cui l'Istituto scolastico ritenga opportuna una presentazione e/o una promozione dell'Istituto scolastico (es. iscrizione nuovo anno scolastico, partecipazione a concorsi, eventi, riconoscimenti), attraverso le visite virtuali dell'Istituto scolastico, le videoconferenze, la comunicazione del materiale a soggetti individuati dall'Istituto scolastico, la pubblicazione sul sito web dell'Istituto e le pagine ufficiali dello stesso sui social media (es. Facebook, Instagram, YouTube), oppure attraverso gli organi di stampa, i media televisivi e ogni altro canale o modalità di comunicazione e il possibile trasferimento dei dati in Paesi non facenti parte dell'Unione come descritto nell'Informativa

□ ESPRIMO IL MIO CONSENSO □ NEGO IL MIO CONSENSO

Nel caso di consenso, DICHIARO anche in riferimento agli artt. 9 e 10 del Codice civile (diritto al nome e all'immagine) e degli artt. 96 e 97 della Legge n. 633/1941 - Legge sul diritto d'autore (diritti relativi al ritratto), di non aver nulla a pretendere, nei confronti della Scuola, in ragione di quanto sopra indicato e di rinunciare irrevocabilmente ad ogni diritto, azione o pretesa derivante da quanto sopra autorizzato. Rimangono salvi i diritti dell'Interessato previsti dal Reg. UE 2016/679 - GDPR (artt. 7 e 15 e seguenti) come indicato nell'Informativa.

Data _____ Firma _____

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.

Si progetta, con la collaborazione dell'assistenza tecnica esterna all'Istituto, un piano di revisione del sistema di filtraggio presente nei vari plessi, così da evitare il più possibile l'accesso a siti inappropriati al contesto scolastico. Per quanto riguarda l'utilizzo di software antivirus si opta per l'utilizzo di programmi gratuiti, scegliendo quelli considerati dal personale tecnico più efficaci. Ai tecnici si affida il compito di mantenere costantemente aggiornati i suddetti software. Tutti coloro che utilizzano i supporti multimediali della scuola saranno sensibilizzati ad eseguire una scansione antivirus quando collegano dispositivi personali di archiviazione esterna. Tutti i plessi dell'Istituto sono dotati di una rete wireless alla quale sono connessi la maggior parte dei dispositivi; ove possibile e conveniente (per es. laboratori di informatica) si procede alla connessione alla rete internet attraverso cavo.
I dispositivi sono collegabili alla rete internet esclusivamente tramite password. Si ritiene utile che il personale docente di ogni plesso, o almeno un rappresentante di essi, sia a conoscenza della password di accesso, così da poter connettere facilmente tutti i dispositivi necessari per lo svolgimento delle attività didattiche.

3.3 - Strumenti di comunicazione online

Le tecnologie digitali sono in grado di ridefinire gli ambienti di apprendimento, supportando la comunicazione a scuola e facilitando un approccio sempre più collaborativo. L'uso degli strumenti di comunicazione online a scuola, al fianco di quelli più tradizionali, ha l'obiettivo di rendere lo scambio comunicativo maggiormente interattivo e orizzontale. Tale uso segue obiettivi e regole precise correlati alle caratteristiche, funzionalità e potenzialità delle tecnologie digitali.

Il personale interno alla scuola (D.S., docenti, personale di segreteria) e i genitori hanno a disposizione la piattaforma di registro elettronico "Nuvola" per comunicazioni "interne". L'Istituto utilizza Google Workspace for Education Fundamentals e Microsoft Office 365.

La Piattaforma Google Workspace for Education Fundamentals è strutturata ed offre un cloud appositamente creato per la scuola che rispetta tutte le norme e le indicazioni del GDPR. Il sistema permette la creazione di account individuali utilizzabili anche da utenti che non abbiano compiuto l'età legale prevista per l'utilizzo di strumenti cloud. Ogni alunno e ogni personale della scuola (Dirigente, docenti, personale ATA) dispongono del proprio account istituzionale con le conseguenti responsabilità che sono collegate ad esso.

La piattaforma dispone di appositi strumenti di comunicazione come:

*Indirizzo di posta elettronica personale di istituto (nome.cognome@iomarsciano.it)

*mailing list di gruppo

*calendario: per una migliore gestione degli impegni e degli eventi

*messaggistica istantanea/chat interna al sistema.

Studenti, docenti e genitori sono informati sul fatto che non è consentito l'utilizzo di strumenti non autorizzati (es. Whatsapp, Instagram, Facebook, messaggistica privata).

Meet, lo strumento per effettuare le videochiamate di gruppo fino a 100 partecipanti, consente di condividere anche lo schermo in modo da poter mostrare l'utilizzo di applicazioni ed è disponibile sia su web oltre che su app per consentire e garantire la massima compatibilità e interoperabilità del sistema.

Il registro elettronico “Nuvola” permette il necessario adempimento amministrativo di rilevazione della presenza in servizio dei docenti e la registrazione della presenza degli alunni a lezione, così come per le comunicazioni scuola-famiglia e l’annotazione delle attività giornaliere e dei compiti. Inoltre è uno strumento che consente la comunicazione tra la scuola e le famiglie. Questa piattaforma permette ai genitori di visualizzare e giustificare le assenze del proprio figlio, visualizzare la bacheca on line, le circolari, l’argomento delle lezioni, i risultati degli scrutini.

- **Sito web della scuola**

Il sito web della scuola (https://salvatorellimoneta.edu.it/) è la prima e principale interfaccia dell’Istituto. Oltre alle informazioni generali e di contatto, vi si trovano apposite sezioni dedicate alle Scuole, ai Servizi, alla Didattica ai Progetti nonchè fondamentali comunicazioni, informazioni, modulistica per docenti, personale ATA alunni e famiglie.

- **Social network**

L’Istituto Omnicomprensivo è attivo sui principali social network, Instagram, Youtube, Facebook, X (Twitter).

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.

La tecnologia, se utilizzata in modo responsabile e corretto, fornisce agli studenti opportunità innovative per incrementare la loro cultura, in linea con quanto specificato nel PNSD. Il nostro Istituto vuole favorire tale processo garantendone la sicurezza attraverso una modalità di interazione che contribuisca al miglioramento dell'ambiente educativo e di apprendimento. Pertanto, l'uso improprio dei dispositivi digitali mobili a scuola non è ammesso e viene sanzionato, in relazione alla gravità dell'infrazione, in base a quanto stabilito dal Regolamento di Istituto.

Sono ammessi a scuola i dispositivi come computer portatile, tablet, e-reader; non sono ammessi cellulari, smartphone, videogiochi in genere.

I dispositivi devono essere usati a scuola per soli scopi didattici e solo con l'autorizzazione dell'insegnante. Agli studenti non è permesso usare dispositivi elettronici per giochi durante le ore scolastiche.

È vietato agli studenti usare dispositivi di registrazione audio, videocamere o fotocamere per registrare video o fare foto in classe senza il permesso dell'insegnante e senza il consenso della persona che viene registrata o ripresa.

Il nostro piano d'azioni

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

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

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

- 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.
- 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 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.*

Il nostro Istituto promuove l'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali, con l'obiettivo di ridurre le situazioni di rischio attraverso azioni che coinvolgono:

1 I docenti:

- Attraverso la formazione personale dei docenti attraverso specifici corsi di aggiornamento offerti dallo stesso Istituto o da Enti qualificati;
- Attraverso l'adesione a progetti dedicati: progetti d'istituto, collaborazione con Convy School, attività proposte da Generazioni connesse.

2 Gli alunni:

- inserimento di ore di educazione alla cittadinanza digitale all'interno del curricolo di Educazione Civica,
- organizzazione di incontri formativi e di attività con i docenti e gli esperti per affrontare i rischi on line nell'arco del loro percorso scolastico;
- l'adesione a progetti dedicati;
- la possibilità di attivare una App della Convy School che permette ai ragazzi di segnalare in forma riservata eventuali problematiche o difficoltà.

3 I Genitori:

- proponendo loro di aderire a progetti specifici con incontri di consulenza da parte di esperti;
- attraverso l'adeguamento del Regolamento d'Istituto e del Patto di Corresponsabilità;
- attraverso colloqui costanti con i docenti del consiglio di classe.

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 nostro Istituto ricorda a tutta la comunità scolastica che gli atti di cyberbullismo possono essere raggruppati in due grandi gruppi:

• **cyberbullismo diretto:** si verifica quando il bullo utilizza strumenti di messaggistica istantanea (es. sms, mms) che hanno un effetto immediato sulla vittima, poiché diretti esclusivamente a lei; come ad esempio nei casi di:

- Flaming: litigi online nei quali si fa uso di un linguaggio violento e volgare;
- Harassment: molestie attuate attraverso l'invio ripetuto di linguaggi offensivi;
- Cyberstalking: invio ripetuto di messaggi che includono esplicite minacce fisiche, al punto che la vittima arriva a temere per la propria incolumità…

• **cyberbullismo indiretto**: si verifica quando il bullo fa uso di spazi pubblici della Rete (es. social network, blog, forum) per diffondere contenuti dannosi e diffamatori per la vittima. Tali contenuti possono diventare virali e quindi più pericolosi per la vittima anche da un punto di vista psicologico. A titolo esemplificativo si possono ricordare:

- Denigrazione: pubblicazione all'interno di comunità virtuali, quali newsgroup, blog, forum di discussione, messaggistica immediata, siti internet … di pettegolezzi e commenti crudeli, calunniosi e denigratori;
- Outing estorto: registrazione delle confidenze, raccolte all'interno di un ambiente privato, creando un clima di fiducia e poi inserite integralmente in un blog pubblico;
- Impersonificazione: insinuazione all'interno dell'account di un'altra persona con l'obiettivo di inviare dal medesimo messaggi ingiuriosi che screditino la

vittima…

E’ inoltre importante ricordare che diventa cyberbullismo anche l’esclusione quando assume una forma di estromissione intenzionale e ripetuta di un individuo dall’attività online. I ragazzi e le ragazze che fanno azioni di bullismo possono commettere reati.

Secondo il codice penale italiano i comportamenti penalmente rilevanti in questi casi sono:

- percosse (art. 581);
- lesione personale (art. 582);
- ingiuria (art. 594);
- diffamazione (art. 595);
- violenza privata (art. 610);
- minaccia (art. 612);
- danneggiamento (art. 635).

Negli atti di bullismo/cyberbullismo vanno distinte le diverse responsabilità ed a tal riguardo si identificano:

1. **Culpa del minore**

Occorre fare una distinzione tra il minore di 14 anni e quello con un’età compresa tra i 14 ed i 18 anni. Il minore di 14 anni non è mai imputabile penalmente. Se viene però riconosciuto come “socialmente pericoloso” possono essere previste misure di sicurezza. Il minore tra i 14 e i 18 anni di età è imputabile se viene dimostrata la sua capacità di intendere e volere. La competenza a determinare la capacità del minore è del giudice che si avvale di consulenti professionali.

2. **Culpa in vigilando ed educando dei genitori**

Si applica l’articolo 2048 del codice civile. Il non esercitare una vigilanza adeguata all’età e indirizzata a correggere comportamenti inadeguati (culpa in educando e vigilando) è alla base della responsabilità civile dei genitori per gli atti illeciti commessi dal figlio minorenne che sia capace di intendere e di volere. A meno che i genitori del minore non dimostrino di non aver potuto impedire il fatto, sono oggettivamente responsabili.

3. **Culpa in vigilando e in organizzando della Scuola**

L’art.28 della Costituzione Italiana recita che “I funzionari ed i dipendenti dello Stato e degli Enti pubblici sono direttamente responsabili, secondo le leggi penali, civili ed amministrative, degli atti compiuti in violazioni di diritti. In tali casi la responsabilità si estende allo Stato ed agli altri enti pubblici.” Dal punto di vista civilistico trova, altresì, applicazione quanto previsto all’Art. 2048 del codice civile, secondo comma, che stabilisce che “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”. La presunzione di colpa può essere superata

solamente laddove si dimostri di aver adeguatamente vigilato ovvero si dia la prova del caso fortuito. Per superare la presunzione, la scuola deve dimostrare di adottare "misure preventive" atte a scongiurare situazioni antigiuridiche.

Al fine di prevenire il fenomeno del cyberbullismo il nostro Istituto ha:

- individuato il referente per la prevenzione e il contrasto del bullismo e del cyberbullismo;
- formato un TEAM di lavoro;
- stimolato un ruolo attivo degli studenti in attività di peer education, cooperative learning e circle time;
- stabilito le procedure di intervento in caso di atti di bullismo/cyberbullismo,
- previsto l'attivazione di uno sportello di ascolto e di aiuto psicologico;
- fissato azioni preventive ed educative e non solo sanzionatorie.

Verranno realizzati progetti sulla base delle esigenze riscontrate, si proporranno attività didattiche ed educative selezionate in base ai fatti compiuti (ampia selezione di materiali è contenuta nell'area del progetto Generazioni Connesse). Verrà richiesta la produzione di lavori scritti/artistici che inducano lo studente a riflettere e rielaborare criticamente gli episodi accaduti, in modo che il bullo possa giungere a un livello di consapevolezza del danno prodotto e la vittima abbia modo di esternare le proprie emozioni.

Gli interventi preventivi ed educativi includono:

- la diffusione e condivisione con gli alunni e le loro famiglie delle iniziative che l'Istituto ha intrapreso, come quelle elencate nel paragrafo precedente;
- l'attuazione di progetti, con l'eventuale contributo esterno di figure professionali, per ampliare le conoscenze digitali degli alunni, creando in loro la consapevolezza dei rischi connessi all'utilizzo della rete;
- i progetti che mirano all'Inclusione, alla valorizzazione delle differenze e valorizzano la gentilezza come forma principale di comunicazione tra pari;
- la formazione ad un uso corretto degli strumenti informatici e l'organizzazione e le regole di utilizzo delle aule di informatica.

Le misure non solo sanzionatorie prevedono:

- attività di natura sociale/culturale che vadano a vantaggio della comunità scolastica: es. svolgimento di azioni positive, quali lettera di scuse a vittima e famiglia, pulizia dei locali, attività di ricerca, riordino materiali, produzione di lavori scritti/artistici che inducano lo studente a riflettere e rielaborare criticamente gli episodi accaduti
- sospensione attiva a scuola, con svolgimento di attività rieducative.

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

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

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

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

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

Il nostro Istituto propone specifiche attività didattiche per fornire agli studenti gli strumenti necessari per contrastare e destrutturare gli stereotipi su cui spesso si fondano forme di hate speech, in particolare legati alla razza, al genere, all'orientamento sessuale, alla disabilità.

Inoltre promuove la partecipazione civica e sensibilizza i ragazzi ad utilizzare il linguaggio della gentilezza, utilizzando anche i materiali messi a disposizione dai siti "Generazioni connesse" e il "manifesto delle parole ostili".

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?

E' ormai diffusa la consapevolezza del ruolo che la tecnologia gioca nella quotidianità dei nostri studenti e dell'impatto che ha sulla qualità della loro vita. Gli elementi che contribuiscono al benessere digitale che possono essere oggetto di riflessione a scuola sono:

• la ricerca di equilibrio nelle relazioni anche online,

• l'uso degli strumenti digitali per il raggiungimento di obiettivi personali,

• la capacità di interagire negli ambienti digitali in modo sicuro e responsabile,

• la capacità di gestire il sovraccarico informativo e le distrazioni (ad esempio, le notifiche).

Da questo punto di vista la didattica può far emergere il potenziale delle nuove tecnologie anche con attività specifiche che facciano emergere la funzionalità dei dispositivi e che al tempo stesso aiutino a prendere consapevolezza rispetto al rischio della dipendenza da Internet.

4.5 - Sexting

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

Il nostro Istituto sta pensando alla possibilità di proporre, nelle classi più a rischio o nelle quali si sono osservate tali esigenze, percorsi di educazione all'affettività e alla sessualità al fine di rendere le alunne e gli alunni 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.

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.

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:

- Promuove la formazione sui rischi dell'adescamento on line durante gli incontri specifici con esperti (forze dell'ordine, polizia postale, psicologa…) rivolti agli studenti, ai genitori e agli insegnanti sul tema della Web reputation e dell'uso improprio delle nuove tecnologie.
- Ricorda che casi di adescamento online richiedono l'intervento delle Forze dell'Ordine:

Polizia di Stato – Compartimento di Polizia postale e delle Comunicazioni;

Questura o Commissariato di P.S. del territorio di competenza;

Arma dei Carabinieri – Comando Provinciale o Stazione del territorio di competenza;

Polizia di Stato – Commissariato on line (attraverso il portale http://www.commissariatodips.it).

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 Istituto affronta il tema della pedopornografia legata al fenomeno del sexting durante gli incontri sui rischi dell'uso improprio delle nuove tecnologie attraverso incontri specifici con esperti (forze dell'ordine, polizia postale, psicologa...) rivolti agli studenti, ai genitori e agli insegnanti.

Casi di pedopornografia richiedono l'intervento delle Forze dell'Ordine:

- Polizia di Stato – Compartimento di Polizia postale e delle Comunicazioni;
- Questura o Commissariato di P.S. del territorio di competenza;
- Arma dei Carabinieri – Comando Provinciale o Stazione del territorio di competenza;
- Polizia di Stato – Commissariato on line (attraverso il portale http://www.commissariatodips.it).

Il nostro piano d'azioni

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

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/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.**

□ 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.

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/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.

☐ **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.

I docenti seguono le procedure standardizzate, presenti in allegato, per la segnalazione e gestione dei problemi connessi a comportamenti online a rischio di studenti e studentesse. Nel caso in cui si ipotizzi che ci si possa trovare di fronte ad una fattispecie di reato come ad esempio, il furto di identità o la persistenza di una condotta persecutoria che mette seriamente a rischio il benessere psicofisico del bambino/a o adolescente coinvolto/a in qualità di vittima si farà riferimento agli uffici preposti delle Forze di Polizia per inoltrare la segnalazione o denuncia/querela e permettere alle autorità competenti l'approfondimento della situazione da un punto di vista investigativo. Si ricorda inoltre che il Garante per la protezione dei dati personali ha pubblicato nel proprio sito il modello per la segnalazione e la rimozione dei contenuti in materia di cyberbullismo da inviare a: cyberbullismo@gpdp.it.

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.

E' opportuno precisare le procedure previste nei due casi sopraccitati.

Nel CASO A, il docente deve:

- avvisare il Coordinatore ed eventualmente l'intero consiglio di classe, coinvolgere il Referente d'Istituto per il contrasto del bullismo e del cyberbullismo valutando insieme le possibili strategie d'intervento, se si ravvisa la necessità e l'urgenza di coinvolgere il Dirigente Scolastico.

Nel frattempo, il docente (in collaborazione con i docenti informati) ascolta gli studenti e le studentesse, osservando e monitorando il clima di classe, ciò che accade, le dinamiche relazionali nel contesto classe, senza fare indagini dirette. Se non si configura un caso di bullismo, è comunque opportuno riflettere sul clima della classe e sulla qualità delle relazioni, utilizzando anche la piattaforma Generazioni Connesse nella parte dei contenuti e dei materiali. Tali attività possono essere molto positive, stimolando il dialogo e la riflessione fra gli studenti e le studentesse. Se gli atti osservati si identificano come atti di bullismo o cyberbullismo, il docente e la scuola tutta devono intervenire seguendo il CASO B.

Nel CASO B, il docente deve:

- condividere immediatamente quanto osservato con il coordinatore di classe e con il referente per il bullismo e il cyberbullismo, valutando insieme le possibili strategie di intervento;
- Avvisare il Dirigente Scolastico che convoca il Consiglio di classe (che applica il "Regolamento di prevenzione e contrasto dei fenomeni di bullismo e cyberbullismo nella scuola") ;

STRUMENTI DI SEGNALAZIONE PREVISTI DALL'ISTITUTO

- indirizzo e-mail specifico per le segnalazioni:

mariangela.severi@iomarsciano.it (Dirigente)

valentina.cruciani@iomarsciano.it (Referente d'istituto per la prevenzione dei fenomi di bullismo e cyberbullismo)

adanella.ranocchia@iomarsciano.it (Docente team prevenzione bullismo)

- scatola/box per la raccolta di segnalazioni anonime;
- attivazione App convy school;
- sportello di ascolto psicologico.

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.

Si elencano gli attori sul territorio:

- **Comitato Regionale Umbria Per L' Unicef**

Viale Roma, 15 (06121 – Perugia)

Lunedì, mercoledì e venerdì
10:00 - 12:00

E-mail comitato.umbria@unicef.it
Tel. e Fax: 075 5849590

- **Ufficio Scolastico Regionale Umbria**

Viale Carlo Manuali, 4 (06121, Perugia)

Tel (+39) 07558281

E-mail direzione-umbria@istruzione.it

PEC drum@postacert.istruzione.it

- **Consultorio casa della salute di Marsciano**

Tel: 0758782405

Indirizzo: Via piccolotti e Cornelli 1

- **Comando Carabinieri di Marsciano**

Indirizzo: Via Vittorio Veneto, 20, 06055 Marsciano PG

Tel: 075 874 2319

- **Polizia Postale e delle Comunicazioni:**

https://www.commissariatodips.it/

- **Polizia postale Perugia**

Via M. Angeloni, 72, 06124 Perugia PG

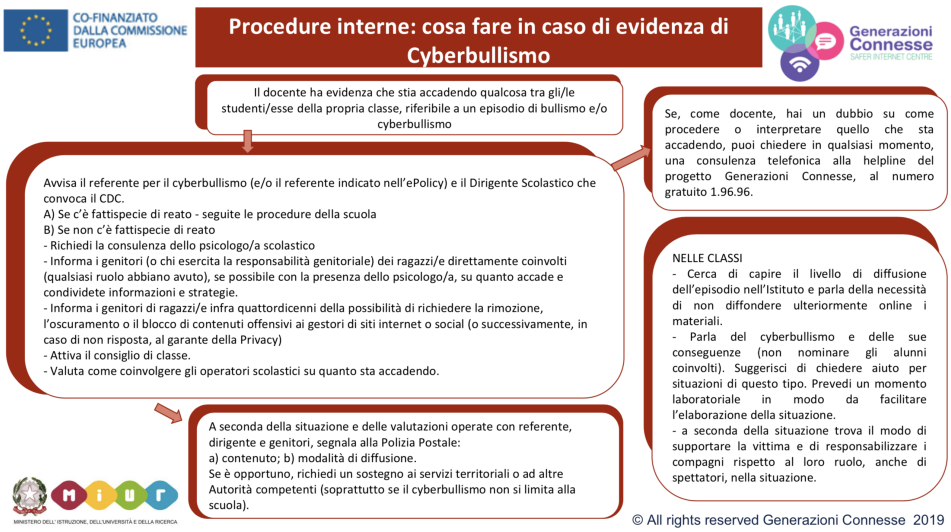
Tel: 0759115311

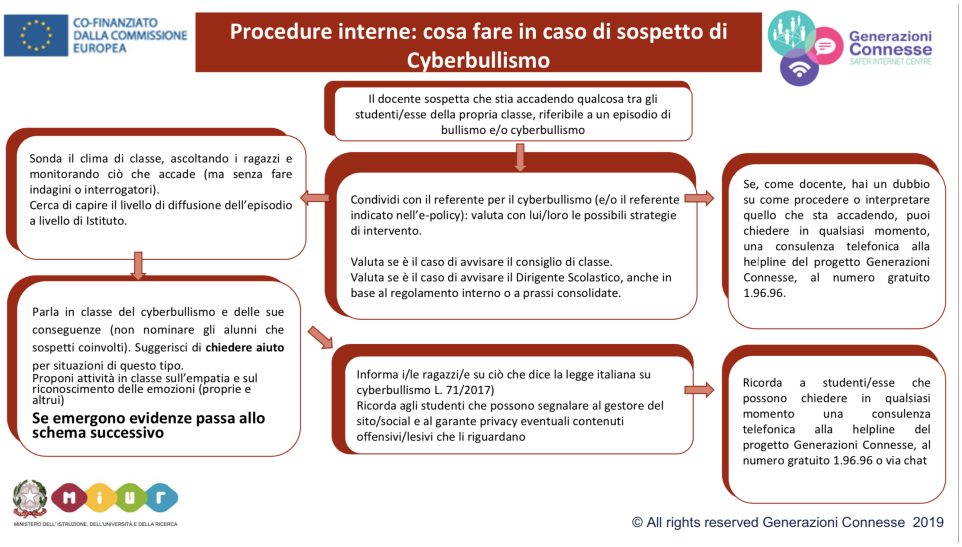
- **Garante per l'infanzia regione Umbria**

garanteminori@regione.umbria.it

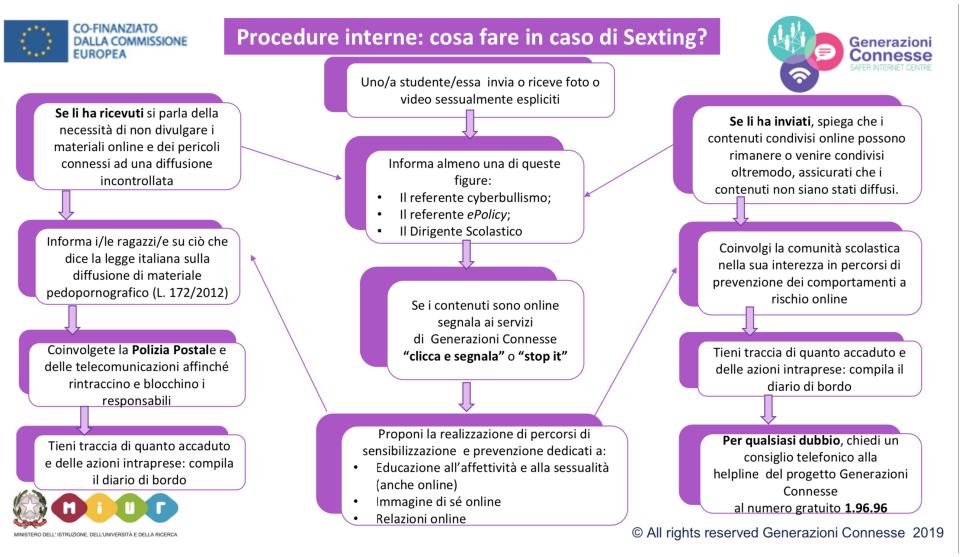
5.4. - Allegati con le procedure

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

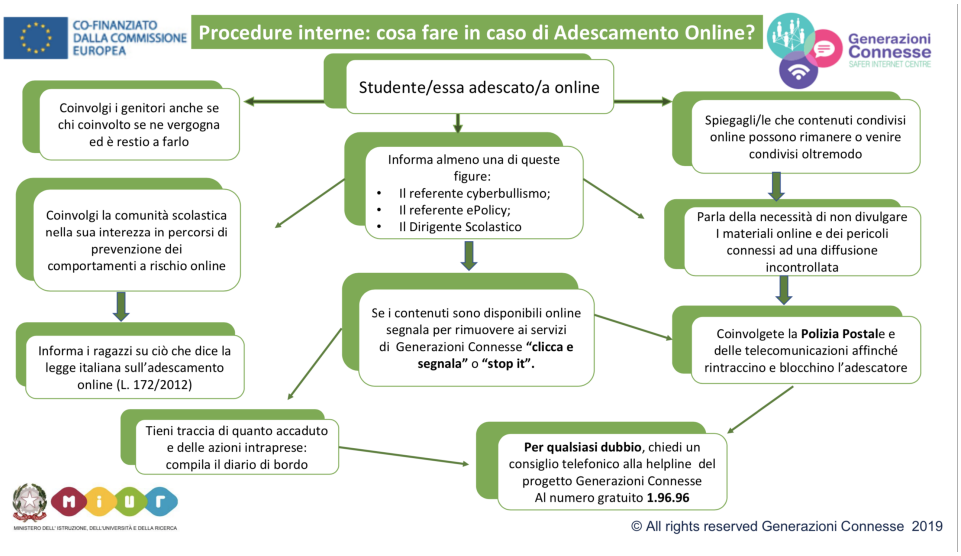




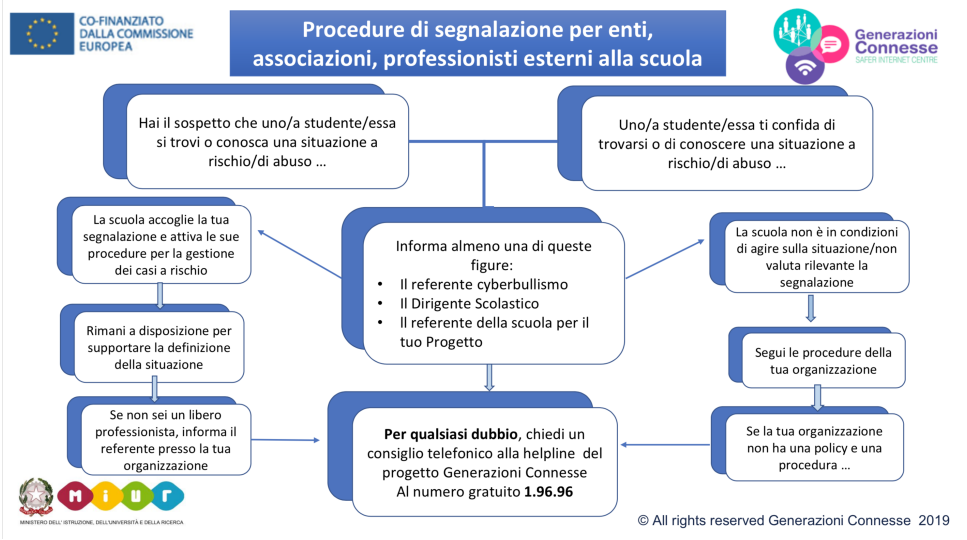
Procedure interne: cosa fare in caso di sexting?



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

Non sono presenti altri allegati

Il nostro piano d'azioni

Nel caso si verificassero i casi esposti si seguiranno le procedure indicate.