Documento di ePolicy

REIC83100N

NOVELLARA

VIA NOVY JICIN 2 - 42017 - NOVELLARA - REGGIO EMILIA (RE)

LUCIA VALENTINI

Capitolo 1 - Introduzione al documento di ePolicy

1.1 - Scopo dell'ePolicy

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

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

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

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

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

Argomenti del Documento

1. **Presentazione dell'ePolicy**
    1. Scopo dell'ePolicy
    2. Ruoli e responsabilità
    3. Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto
    4. Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica

5. Gestione delle infrazioni alla ePolicy
6. Integrazione dell'ePolicy con regolamenti esistenti
7. Monitoraggio dell'implementazione dell'ePolicy e suo aggiornamento

2. **Formazione e curricolo**
    1. Curricolo sulle competenze digitali per gli studenti
    2. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica
    3. Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali
    4. Sensibilizzazione delle famiglie e Patto di corresponsabilità
3. **Gestione dell'infrastruttura e della strumentazione ICT (Information and Communication Technology) della e nella scuola**
    1. Protezione dei dati personali
    2. Accesso ad Internet
    3. Strumenti di comunicazione online
    4. Strumentazione personale
4. **Rischi on line: conoscere, prevenire e rilevare**
    1. Sensibilizzazione e prevenzione
    2. Cyberbullismo: che cos'è e come prevenirlo
    3. Hate speech: che cos'è e come prevenirlo
    4. Dipendenza da Internet e gioco online
    5. Sexting
    6. Adescamento online
    7. Pedopornografia
5. **Segnalazione e gestione dei casi**
    1. Cosa segnalare
    2. Come segnalare: quali strumenti e a chi
    3. Gli attori sul territorio per intervenire
    4. Allegati con le procedure

Perché è importante dotarsi di una E-policy?

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

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

In particolare l'intento del nostro Istituto comprensivo è quello di promuovere l'uso consapevole e critico da parte degli alunni delle tecnologie digitali (TIC) e di Internet, di far acquisire loro

procedure e competenze tecniche ma anche corrette norme comportamentali per prevenire e fronteggiare le problematiche che derivano da un utilizzo non responsabile, pericoloso e/o dannoso delle tecnologie digitali.

Attraverso l'Epolicy 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 consapevole, critico ed efficace e per sviluppare, attraverso specifiche azioni, la conoscenza delle opportunità e dei rischi connessi all'uso di Internet.

I principi fondamentali sono:

- salvaguardare e proteggere i bambini, i ragazzi e tutto il personale dell'Istituto;
- impostare norme di condotta rilevanti per un uso responsabile di Internet a scopo didattico, personale o ricreativo;
- garantire che tutti i membri della comunità scolastica siano consapevoli del fatto che il comportamento illecito o pericoloso è inaccettabile e che saranno intraprese le opportune azioni disciplinari e/o giudiziarie.

1.2 - Ruoli e responsabilità

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

Il Dirigente Scolastico

Il Dirigente Scolastico garantisce la sicurezza, anche online, di tutti i membri della comunità scolastica: in quest'ottica, è formato adeguatamente sulla sicurezza e sulla prevenzione di problematiche offline e online, in linea con il quadro normativo di riferimento e le indicazioni del MIUR.

Promuove la cultura della sicurezza online e, ove possibile, dà il proprio contributo all'organizzazione, insieme al docente referente sulle tematiche del bullismo/cyberbullismo e al docente funzione strumentale per l'Area Digitale dell'IC, di corsi di formazione specifici per tutte le figure scolastiche sull'utilizzo positivo e responsabile delle TIC.

Infine, il Dirigente Scolastico ha la responsabilità di gestire e intervenire nei casi di gravi episodi di bullismo, cyberbullismo e uso improprio delle tecnologie digitali.

L'Animatore digitale

L'Animatore digitale supporta il personale scolastico da un punto di vista non solo tecnico-informatico, ma anche in riferimento ai rischi online, alla protezione e gestione dei dati personali, oltre che essere uno dei promotori di percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale" (con riferimento, ad esempio, allo sviluppo delle competenze digitali previste anche nell'ambito dell'educazione civica); inoltre, monitora e rileva eventuali episodi o problematiche connesse all'uso delle TIC a scuola e ha il compito di controllare che gli utenti autorizzati accedano alla Rete della scuola con apposita password, per scopi istituzionali e consentiti (istruzione e formazione).

Il Referente bullismo e cyberbullismo

"Ogni Istituto scolastico, nell'ambito della propria autonomia, individua fra i docenti un referente con il compito di coordinare le iniziative di prevenzione e di contrasto del cyberbullismo" (Art. 4 Legge n.71/2017, "Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo" (permalink – file 1 LEGGE 71_2017 in allegato).

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

I Docenti

I Docenti hanno un ruolo centrale nel diffondere la cultura dell'uso responsabile delle TIC e della Rete. Innanzi tutto, integrano parti del curriculum della propria disciplina con approfondimenti specifici, promuovendo, laddove possibile, anche l'uso delle tecnologie digitali nella didattica. I docenti accompagnano e supportano gli studenti e le studentesse nelle attività di apprendimento e nei laboratori che prevedono l'uso della LIM o di altri dispositivi tecnologici che si connettono alla Rete; hanno il dovere morale e professionale di segnalare al Dirigente Scolastico qualunque problematica, violazione o abuso, anche online, che vede coinvolti studenti e studentesse.

Il personale Amministrativo, Tecnico e Ausiliario (ATA)

Il personale Amministrativo, Tecnico e Ausiliario (ATA) svolge funzioni miste, ossia di tipo amministrativo, contabile, gestionale e di sorveglianza connesse all'attività delle istituzioni

scolastiche, in collaborazione con il dirigente scolastico e con il personale docente tutto. Diverse figure che, in sinergia, si occupano ciascuno per la propria funzione, del funzionamento dell'Istituto scolastico che passa anche attraverso lo sviluppo della cultura digitale e dell'organizzazione del tempo scuola. Esiste, cioè, un concreto coinvolgimento del personale ATA nell'applicazione della legge 107/15 ("La Buona Scuola") che concerne non solo il tempo scuola e il potenziamento dell'offerta formativa, ma anche le attività di formazione e autoformazione in tema di bullismo e cyberbullismo.

Il personale ATA, all'interno dei singoli regolamenti d'Istituto, viene coinvolto nella segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo, insieme ad altre figure e nella raccolta, verifica e valutazione delle informazioni inerenti possibili casi di bullismo/cyberbullismo.

Gli Studenti e le Studentesse

Gli Studenti e le Studentesse, in relazione al proprio grado di maturità e consapevolezza raggiunta, si impegnano a utilizzare al meglio le tecnologie digitali in coerenza con quanto richiesto dai docenti; con il supporto della scuola imparano a tutelarsi online, a tutelare i/le propri/e compagni/e e rispettarli/le; sono chiamati a partecipare attivamente a progetti e attività che riguardano l'uso positivo delle TIC e della Rete e a farsi promotori di quanto appreso, anche attraverso possibili percorsi di *peer education*.

I Genitori

I Genitori, in continuità con l'Istituto scolastico, sono coinvolti nella partecipazione alle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete, nonché sull'uso responsabile dei device personali; sono chiamati a relazionarsi in modo costruttivo con i docenti sulle linee educative che riguardano le TIC e la Rete e a comunicare con loro circa i problemi rilevati quando i/le propri/e figli/e non usano responsabilmente le tecnologie digitali o Internet. È estremamente importante che accettino e condividano quanto scritto nell'ePolicy dell'Istituto.

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

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.

Nello specifico il testo sarà condiviso con:

- studenti e studentesse per dare loro: una base di partenza per l'uso consapevole e maturo dei dispositivi e della tecnologia informatica; regole condivise di sicurezza circa il comportamento da tenere a scuola e nei conesti extrascolastici; elementi per poter riconoscere e prevenire comportamenti a rischio sia personali che dei compagni;
- personale scolastico per poter orientare tutte le figure sui temi in oggetto, a partire da un uso corretto dei dispositivi e della rete;
- genitori sul sito istituzionale della scuola e/o tramite momenti di formazione specifici durante gli incontri scuola-famiglia.

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.

L'Istituto interviene seguento un preciso *iter*:

- richiamo verbale;
- sanzioni estemporanee commisurate alla gravità della violazione commessa (per esempio assegnazione di attività aggiuntive da svolgere a casa sui temi di Cittadinanza e Costituzione);
- nota informativa ai genitori o ai tutori mediante registro elettronico;
- convocazione dei genitori o tutori per un colloquio con l'insegnante;
- convocazione dei genitori o tutori per un colloquio con il Dirigente Scolastico;
- denunce di cyberbullismo saranno trattate in conformità con il Regolamento d'Istituto in primis ed eventualmente con quanto stabilito dalla legge.

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.

La presente E-policy Safety verrà pubblicata sul sito della scuola per informare anche i genitori, visto che anche la loro condotta può favorire l'uso corretto e responsabile delle TIC da parte degli alunni a scuola.

Le situazioni familiari meno favorevoli sono:

- la convinzione che se il proprio figlio rimane a casa a usare il computer è al sicuro;
- una piena autonomia concessa al proprio figlio nella navigazione sul web e nell'utilizzo del cellulare senza un periodico controllo dei contenuti;
- la mancanza di adeguata conoscenza che la responsabilità dei contenuti dello smartphone dei minori è sempre ascrivibile ai genitori/tutori.

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 referente di bullismo e cyberbullismo, affiancato dal Team Digitale dell'IC, controlla che l'E-policy sia aggiornata in merito alle novità emergenti a livello normativo e non riguardanti l'uso consapevole delle TIC; valuta che gli obiettivi prefissi siano raggiunti ed eventualmente riacalibrati rispetto ai destinatari, per programmare interventi formativi e attività specifiche.

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 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 incontri per la consultazione degli studenti/studentesse sui temi dell'ePolicy per cui si evidenzia la necessità di regolamentare azioni e

comportamenti

- 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

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.

Per livelli diversi di applicazione in riferimento alle esigenze delle classi e dei singoli alunni, l'Istituto Comprensivo propone un Curricolo Digitale che abbraccia nel percorso scolastico di tutto il 1^ ciclo di istruzione le aree di competenza del Framework e fornisce indicazioni per lo sviluppo delle attività individuate dai docenti.

Il documento, redatto dai componenti dell'Area Digitale a seguito delle esperienze dell'IC relative al PNSD ed elaborato sulla necessità di sperimentare nuove metodologie e risorse didattiche, si propone come uno strumento di lavoro aperto a modifiche e implementazioni in itinere, anche in relazione alla DDI e alle esigenze contingenti che chiamano in causa le TIC.

Poiché queste ultime e il mondo a esse collegato sono in continua e rapida evoluzione, non si ritiene utile delimitare entro confini metodologici e contenutistici le possibilità offerte dal digitale nella didattica: in quest'ottica, l'elenco si propone un ricco elenco di attività, un bacino di suggerimenti e indicazioni operative volte a promuovere nei docenti la sperimentazione e la ricerca didattica.

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.

L'Istituto propone ai docenti percorsi formativi finanziati dal PNSD, nello specifico su:

- coding
- tinkering
- realtà aumentata
- realtà virtuale
- G-Suite per la didattica
- lingua inglese

A questo pacchetto formativo, si affianca la formazione offerta dal Team Digitale, in particolare sui dispositivi e la dotazione informatica della scuola e sugli strumenti digitali in uso (registro elettronico e applicazioni connesse all'indirizzo mail istituzionale); i componenti del Team sono a disposizione anche per un periodico servizio di "sportello digitale" (via Meet), che supporta i colleghi nella pratica didattica ordinaria e nella sperimentazione 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.

L'Istituto aggiorna periodicamente, mediante comunicazioni via mail, pubblicazioni sul sito e momenti dedicati nelle riunioni del Collegio, gli insegnanti rispetto alla normativa riguardante l'uso corretto e consapevole della rete in ambito scolastico ed extrascolastico, avvalendosi della consulenza del DPO; promuove iniziative formative dedicate, anche in collaborazione con l'Ente Locale e le agenzie del territorio.

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'IC aggiorna - compatibilmente con le esigenze organizzative, in modo il più possibile tempestivo - rispetto alla normativa, alle modifiche nell'informativa per l'uso delle TIC a scuola e alle iniziative intraprese rispetto al digitale, all'uso corretto della rete e degli strumenti informatici. In particolare, il Patto Educativo di Corresponsabilità è stato aggiornato con una Netiquette, di seguito riportata:

- rispettare le persone diverse per nazionalità, cultura, religione, sesso;
- non essere intolleranti con chi ha scarsa dimestichezza con le TIC o commette errori concettuali;
- non rivelare dettagli o informazioni personali o di altre persone (indirizzi, e-mail, numeri di telefono);
- non inviare fotografie proprie o di altre persone;
- riferire sempre a insegnanti e genitori se si incontrano in internet immagini o scritti che infastidiscono;
- se qualcuno non rispetta queste regole è opportuno parlarne con gli insegnanti o con i genitori;

- chiedere il permesso prima di scaricare dal web materiale di vario tipo.

Anche nella navigazione al di fuori del contesto scolastico è bene che gli alunni mantengano comportamenti corretti e responsabili, quali:

- non iscriversi autonomamente a mailing-list o a siti web che lo richiedano;
- non dare mai indirizzo e numero di telefono a persone incontrate sul web, e avvertire immediatamente i propri genitori;
- non prendere mai appuntamenti con le persone conosciute tramite web se avvertire immediatamente i propri genitori.

Il nostro piano d'azioni

AZIONI da sviluppare nell'arco dell'anno scolastico 2020/2021:

- Coinvolgere una rappresentanza dei genitori per individuare i temi di maggiore interesse nell'ambito dell'educazione alla cittadinanza digitale.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.

AZIONI da sviluppare nell'arco dei tre anni scolastici successivi:

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

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

3.1 - Protezione dei dati personali

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

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

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

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

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

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

personali.

Nell'ottica di ampliare l'offerta formativa, incrementare la dematerializzazione delle risorse, esplorare nuove modalità di comunicazione, educare a un uso consapevole e responsabile di internet e fornire una adeguata alfabetizzazione informatica di base ai propri studenti, l'Istituto Comprensivo NOVELLARA ha deciso di avvalersi dei servizi della piattaforma GSuite for Education.

I servizi a disposizione dell'Istituto comprendono:

- Gmail, per l'assegnazione di casella di posta con spazio illimitato;
- Calendar, per la gestione dell'agenda;
- Classroom, per la creazione e gestione di classi virtuali; -
- Drive, per l'archiviazione e condivisione dei documenti;
- Documenti, Moduli, Fogli, Presentazioni, per la creazione e condivisione di materiale didattico;
- Talk/Hangouts, per permettere di stabilire comunicazioni in tempo reale e creare webinar;
- Servizi aggiuntivi (es. Youtube, Blogger) che possono essere utilizzati per scopi didattici anche con account G Suite for Education.

Il titolare del trattamento è Istituto Comprensivo Statale di Novellara, con sede in Via Novy Jicin 2, 42017-Novellara (RE), C.F. 81000500355, in persona del legale rappresentante Lucia Valentini: e-mail reic83100n@istruzione.it , pec reic83100n@pec.istruzione.it, telefono +39 0522 654218.

Il responsabile della protezione dei dati è Corporate Studio S.r.l., C.F./P. IVA: 02480300355, in persona del legale rappresentante pro tempore, con sede in Reggio Emilia, via Brigata Reggio n. 28, e-mail privacy@corporatestudio.it, pec corporatestudiore@pec.it.

3.2 - Accesso ad Internet

1. *L'accesso a Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale.*
2. *Ogni persona ha eguale diritto di accedere a Internet in condizioni di parità, con modalità tecnologicamente adeguate e aggiornate che rimuovano ogni ostacolo di ordine economico e sociale.*
3. *Il diritto fondamentale di accesso a Internet deve essere assicurato nei suoi presupposti sostanziali e non solo come possibilità di collegamento alla Rete.*
4. *L'accesso comprende la libertà di scelta per quanto riguarda dispositivi, sistemi operativi e applicazioni anche distribuite.*
5. *Le Istituzioni pubbliche garantiscono i necessari interventi per il superamento di ogni forma di divario digitale tra cui quelli determinati dal genere, dalle condizioni economiche oltre che*

da situazioni di vulnerabilità personale e disabilità.

Così recita l'art. 2 della Dichiarazione dei diritti di Internet, elaborata dalla Commissione per i diritti e i doveri in Internet, commissione costituita il 27 ottobre 2014 presso la Camera dei Deputati dalla presidente Laura Boldrini e presieduta da Stefano Rodotà. Inoltre, il 30 aprile 2016 era entrato in vigore il Regolamento UE del Parlamento Europeo e del Consiglio del 25 novembre 2015, che stabilisce le "misure riguardanti l'accesso a un'Internet aperto e che modifica la direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica e il regolamento (UE) n. 531/2012 relativo al roaming sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione".

Il diritto di accesso a Internet è dunque presente nell'ordinamento italiano ed europeo e la scuola dovrebbe essere il luogo dove tale diritto è garantito, anche per quegli studenti che non dispongono della Rete a casa. In modo coerente il PNSD (Piano Nazionale Scuola Digitale) ha tra gli obiettivi quello di "fornire a tutte le scuole le condizioni per l'accesso alla società dell'informazione e fare in modo che il "diritto a Internet" diventi una realtà, a partire dalla scuola".

Questo perché le tecnologie da un lato contribuiscono a creare un ambiente che può rendere la scuola aperta, flessibile e inclusiva, dall'altro le consentono di adeguarsi ai cambiamenti della società e del mercato del lavoro, puntando a sviluppare una cultura digitale diffusa che deve iniziare proprio a scuola.

L'Istituto ha elaborato e condiviso con studenti e docenti un "Regolamento per l'uso delle dotazioni tecnologiche, di rete e Internet" nel quale si stabiliscono le regole di comportamento da rispettare per l'utilizzo dei dispositivi presenti nei plessi.

Per accedere a Internet dai locali della scuola secondaria di 1^ grado "L. Orsi" e della scuola primaria "Don Milani" è necessario autenticarsi tramite le credenziali (nome utente e password) di Federa. Ciò permette di tracciare la navigazione in Internet delle persone connesse, sia docenti che alunni, consentendo al Dirigente Scolastico di poter comunicare alla Polizia Postale, in caso di necessità, l'identità delle persone collegate a Internet in qualsiasi momento dai computer delle due sedi e tutti i siti visitati durante la navigazione (conoscenze previste dalla legge). Grazie a questo tipo di controllo, gli utenti sono fortemente disincentivati a compiere azioni sconvenienti durante la navigazione in Internet (hackeraggio, cyberbullismo, navigazione in siti non inerenti l'attività didattica ecc…).

La connessione a Internet tramite le credenziali Federa fornite dall'Istituto Comprensivo di Novellara può avvenire solamente dai locali delle sedi "L. Orsi" e "Don Milani" (non tramite Hot Spot sul territorio) e consente inoltre di attivare un filtro di navigazione che limita l'accesso a siti con contenuti inadeguati per i ragazzi delle scuole.

Fermo restando che la responsabilità sull'attività svolta in rete dagli alunni durante l'orario scolastico è comunque dei docenti a cui sono affidati, Federa richiede, per l'assegnazione delle credenziali agli alunni minorenni, il consenso da parte della famiglia tramite la firma di un modulo predisposto e la consegna, insieme al modulo compilato e firmato da parte di un genitore, della

fotocopia di un documento di identità.

3.3 - Strumenti di comunicazione online

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

L'Istituto garantisce la comunicazione con genitori, insegnanti e alunni tramite diversi canali:

- Sito dell'Istituto: pubblicazione di avvisi, circolari, iniziative ed eventi;
- Registro Elettronico Nuvola: accesso con autenticazione dei genitori per verificare l'andamento dello studente, per visualizzare i compiti assegnati o per prenotare i colloqui individuali con i docenti. Inoltre le famiglie possono accedere al documento di valutazione periodico e finale e scaricarlo sul loro dispositivo;
- Email personali dei tutori: per comunicazioni personali e invio di comunicazioni importanti;
- GSuite: gli studenti e il personale docente sono provvisti dalla scuola di indirizzo email istituzionale (@icnovellara.edu.it) che gli permette di accedere alla piattaforma per svolgere attività didattiche proposte dai docenti.

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.

L'Istituto possiede diversi dispositivi tecnologici (tra questi, LIM, tablet, Chromebook) che vengono utilizzati e integrati nella didattica quotidiana. Alcuni di questi dispositivi, in caso di necessità, possono essere dati in comodato d'uso gratuito a tutti gli studenti che non hanno device adatti per poter svolgere le attività scolastiche. La scuola sta predisponendo le modalità e la regolamentazione per l'adozione del BYOD rispetto ad alcune attività didattiche.

Il nostro piano d'azioni

AZIONI da sviluppare nell'arco dell'anno scolastico 2020/2021:

- Organizzare incontri per la consultazione dei genitori su indicazioni/regolamentisull'uso dei dispositivi digitali personali
- Organizzare uno o più eventi o attività volti a formare i genitori dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali

AZIONI da sviluppare nell'arco dei tre anni scolastici successivi:

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

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

4.1 - Sensibilizzazione e Prevenzione

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

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

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

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

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

La necessità di sensibilizzare gli studenti a un uso sicuro e consapevole delle tecnologie, sia in un'ottica di tutela dei rischi potenziali che di valorizzazione delle opportunità esistenti, pone tutta la comunità educante di fronte alla sfida di riconsiderare la propria identità, le proprie risorse e il proprio ruolo educativo.

Il nostro Istituto Comprensivo intende perseguire azioni di prevenzione universale e di sensibilizzazione attraverso un'efficace integrazione con i servizi territoriali locali (Comune, ASL, Forze dell'Ordine...) al fine di formare e consolidare quelle competenze educative di base necessarie per poter gestire le situazioni che i ragazzi sperimentano online.

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).

Per sensibilizzare gli studenti al fenomeno del bullismo e del cyberbullismo, è innanzitutto necessario fornire loro i tratti salienti dei 2 fenomeni affinché possano riconoscerli e difendersi.

Si parla di bullismo quando si verificano situazioni caratterizzate da volontarie e ripetute aggressioni mirate a insultare, minacciare, diffamare e/o ferire una parsona; si tratta pertanto di comportamenti ripetuti nel tempo. Quando queste vessazioni vengono fatte online, si parla di cyberbullismo.

Questo fenomeno ha le seguenti caratteristiche:

- è invasivo: il bullo può raggiungere la vittima in qualsiasi momento e in qualsiasi luogo;
- è persistente: il materiale messo online può rimanere per molto tempo e propagarsi molto velocemente;
- ha una platea potenzialmente infinita: le persone che possono assistere agli atti di cyberbullismo sono potenzialmente illimitate.

A seconda dei casi si potranno adottare azioni di prevenzione universale, sellettiva e indicata.

1. Prevenzione universale: un programma di questo tipo parte dal presupposto che tutti gli studenti siano potenzialmente a rischio.
2. Prevenzione selettiva: un programma dedicato a un gruppo di studenti in cui il rischio online è presente. In questo caso la presenza del rischio è stata individuata attraverso segnalazioni fatte dalla vittima alla scuola o ad un insegnante e successive indagine di approfondimento.
3. Prevenzione indicata: un programma di intervento sul caso specifico, pensato quindi per ridurre comportamenti problematici o dare supporto alle vittime.

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.

Lo sviluppo delle competenze digitali e l'educazione a un uso consapevole delle tecnologie assumono un ruolo centrale anche per prevenire queste dinamiche in rete.

Occorre pertanto valorizzare la dimensione relazionale e formire agli studenti gli strumenti necessari per decostruire gli stereotipi su cui si fondano forme di *hate speech*, in particolare legati alla razza, all'orientamento sessuale, alla disabilità.

L'Istituto intende quindi avvalersi di consulenti/esperti esterni per organizzare incontri informativi e informativi per sensibilizzare al problema (Carabinieri, Polizia Postale, associazioni del territorio preposte allo scopo, psicologa scolastica).

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?

Anche in questo caso, la scuola ha la possibilità di fare formazione e di indicare strategie per un uso più consapevole delle tecnologie e per favorire il "benessere digitale", cioè la capacità di mantenere una relazione sana con la tecnologia.

Partendo dal presupposto che la tecnologia ha modificato gli ambienti in cui viviamo e che ha un impatto sulla qualità della vita, è necessario far conoscere agli studenti quali sono gli elementi che contribuiscono al "benessere digitale":

- la ricerca di equilibrio anche nelle relazioni 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.

Ci si propone pertanto di lanciare un messaggio preciso: se controlliamo la tecnologia, possiamo usarne il pieno potenziale e trarne vantaggi, attenendoci a regole condivise.

Il nostro Istituto intende dare informazioni riguardo ai comportamenti a rischio; nel caso specifico della dipendenza da Internet e del gioco online, far capire che ciò rappresenta una vera e propria patologia che compromette la salute e le relazioni sociali.

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.

A questo proposito è opportuno parlare con gli studenti di temi legati alla sessualità, all'affettività e alle differenze di genere.

Bisogna informare i giovani, ricordando loro che la detenzione e l'invio di foto che ritraggono minorenni in pose sessualmente esplicite configura il reato di distribuzione di materiale pedopornografico.

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.

Grazie alla collaborazione con le Forze dell'Ordine, l'Istituto propone un'azione di sensibilizzazione sull'esistenza di individui che usano la rete per instaurare relazioni, virtuali o reali, con minorenni per indurli alla prostituzione nei casi più gravi.

Perciò è fondamentale far comprendere la nozione basilare secondo cui la propria e altrui sicurezza in rete non dipende solo dalla tecnologia adottata, ma anche dalla capacità di discernimento delle singole persone nel proprio relazionarsi attraverso la rete.

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.

In un'ottica di attività preventiva, il tema della pedopornografia è estremamente delicato. Occorre pertanto parlarne considerando la maturità, la fascia d'età e selezionando le informazioni che si

possono condividere

Risulta utilissima l'attività educativa sull'affettività e le relazioni, sottolineando sempre la necessità di rivolgersi ad un adulto quando qualcosa online mette a disagio.

Il nostro piano d'azioni

AZIONI da sviluppare nell'arco dell'anno scolastico 2020/2021:

□ Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti agli studenti e ai genitori.

□ 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.

AZIONI da sviluppare nell'arco dei tre anni scolastici successivi:

□ 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 eventi e/o dibattiti in momenti extra-scolastici, sui temi della diversità e sull'inclusione rivolti a genitori, studenti/studentesse e personale della 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.

Si considerano da segnalare tutte quelle situazioni caratterizzate da volontarie e ripetute aggressioni mirate a insultare, minacciare, diffamare una persona tramite l'uso di internet.

Partendo dal presupposto che il nostro Istituto intende prevenire e contrastare qualsiasi forma di

bullismo e di cyberbulismo, l'offerta formativa viene integrata con attività specifiche afferenti a Cittadinanza e Costituzione per tradurre i "saperi" in comportamenti consapevoli e corretti che stanno alla base della convivenza civile. Si organizzano pertanto incontri formativi e informativi tenuti da esperti e dall'Arma dei Carabinieri sui fenomeni del bullismo e del cyberbullismo, oltre all'apertura di uno sportello d'ascolto con la psicologa scolastica a cui gli studenti possono rivolgersi per avere consigli o sostegno psicologo. Lo sportello si articola in colloqui individuali, al fine di migliorare il benessere personale e scolastico, mediante un'attività di supporto della sfera emotiva, relazionale e comportamentale. In tutto ciò rimane comunque presente anche la figura dell'insegnante che può essere un adulto di cui ci si fida o il referente al bullismo/cyberbullismo.

Accorgersi tempestivamente di quanto accade e compiere immediatamente azioni di contrasto verso gli atti inopportuni è fondamentale per poter evitare conseguenze a lungo termine che possano pregiudicare il benessere dei soggetti coinvolti.

Gli interventi che la scuola metterà in atto saranno tesi a far conoscere e a sensibilizzare gli alunni verso un uso responsabile della rete, al fine di assicurare loro il rispetto del diritto a essere tutelati da abusi da un lato e, allo stesso tempo, suscitare atteggiamenti di rispetto verso gli altri utenti.

La scuola avrà quindi cura di porre attenzione alla rilevazione dei rischi connessi alla navigazione sul web. In particolare si segnaleranno:

- contenuti afferenti alla violazione della privacy (foto personali, l'indirizzo di casa o il numero di telefono,informazioni private, foto o viedo pubblicate contro la propria volontà ecc...)
- contenuti afferenti all'aggressività o alla violenza (messaggi minacciosi, commenti offensivi, foto o video imbarazzanti, false informazioni, pettegolezzi, insulti, contenuti razzisti ecc...)
- contenuti afferenti alla sessualità: messaggi molesti, foto o video personali con nudità o abbigliamento succinto, immagini pornografiche, foto e video in cui minori sono coinvolti o assistono ad attività sessuali (pedopornografia).

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.

Nella segnalazione e nella gestione dei casi, la scuola opererà una politica di intervento sia reattiva che pro-attiva. Quella reattiva dovrà prevedere azioni di supporto al (cyber)bullo affinché possa arrivare a comprendere che qualsiasi forma di sopraffazione non è accettabile; la proattiva richiede la partecipazione di tutte le componenti della comunità scolastica e dovrà essere rivolta a insegnare a tutti, potenziali bulli e vittime, a gestire la propria aggressività, promuovendo un'interazione tra pari più responsabile.

Le procedure interne per la rilevazione e la gestione dei casi, nonchè la segnalazione al Dirigente scolastico ed eventualmente alle autorità competenti avvengono secondo i protocolli suggeriti dalla piattaforma di "Generazioni connesse", come da schemi allegati. Il personale docente in particolare è quindi chiamato a osservare per tempo ciò che accade, condividendo ogni episodio a livello di Consiglio di Classe, che potrà decidere di applicare eventuali sanzioni. Alcuni casi di lieve rilevanza possono essere affrontati con la discussione collettiva in classe e/o un lavoro interdisciplinare *ad hoc* sul fenomeno (cyber)bullismo. Altri casi possono essere affrontati convocando genitori e alunno/a per riflettere insieme sull'accaduto e individuare una strategia comune per affrontarlo e cercare di risolverlo. Per i casi più gravi, bisogna invece informare il Dirigente Scolastico che qualora di fronte

a reati veri e propri effettuerà la denuncia all'autorità giudiziaria. Quale che sia la gravità, è opportuno informare sempre le famiglie sia del (cyber)bullo che della vittima e cercare di ottenere prove oggettive per la ricostruzione dell'accaduto.

La scuola si occuperà di organizzare interventi *ad hoc* grazie alla collaborazione con l'Arma dei Carabinieri che, con l'elenco di tutti i possibili reati e le relative sanzioni, sono finalizzati a creare un clima di solidarietà, a combattere l'indifferenza, a incoraggiare le vittime a chiedere aiuto e a sottrarre al (cyber)bullo potenziali proseliti.

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.

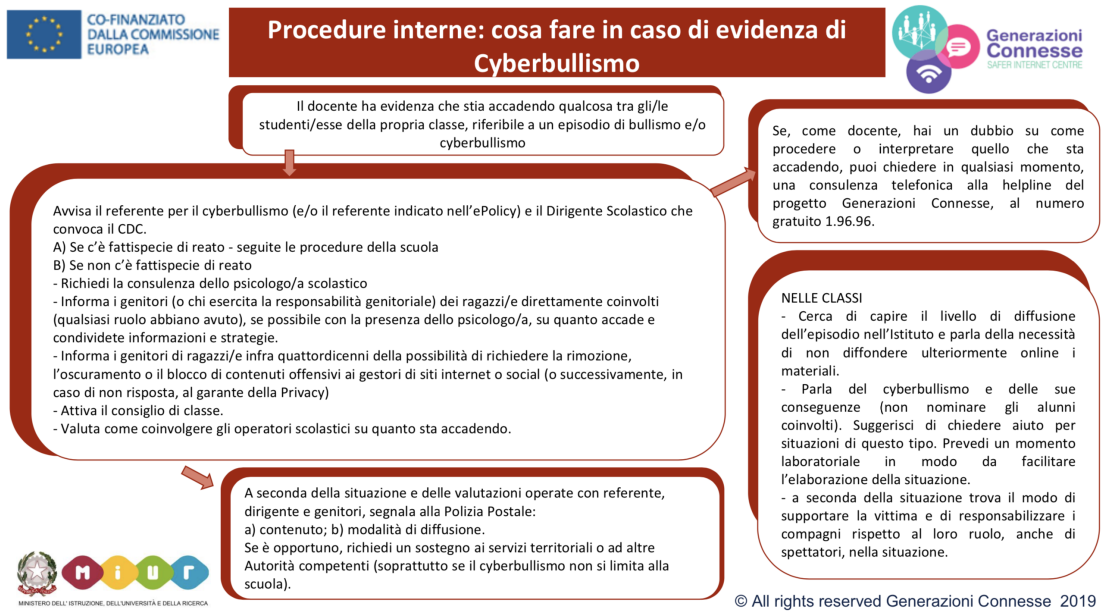
- **Tribunale per i Minorenni**: segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

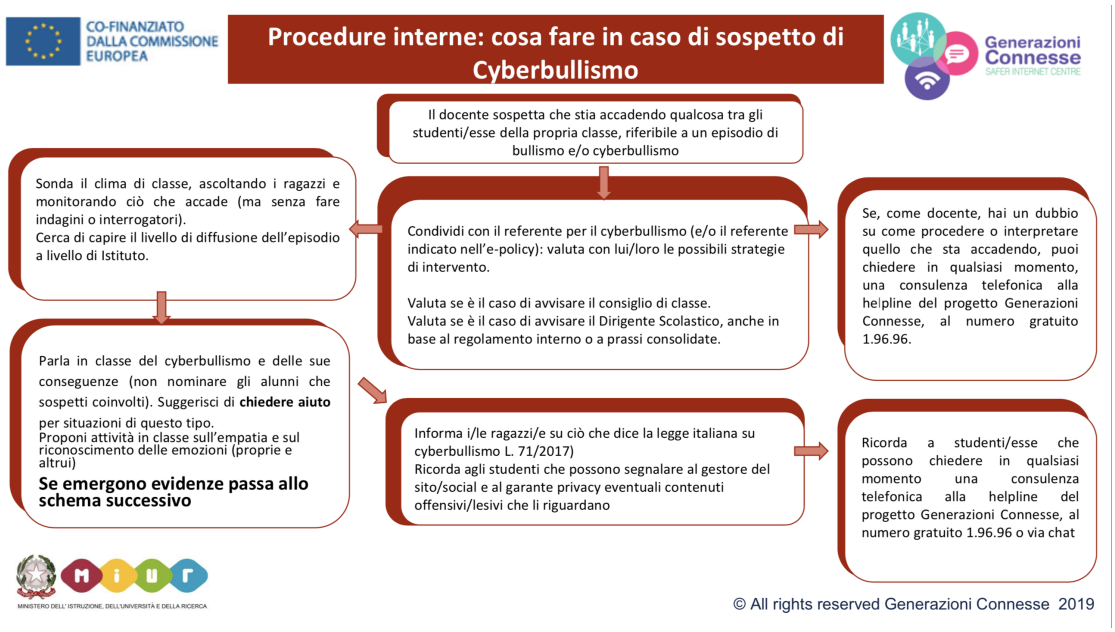
Al fine di contrastare il fenomeno del (cyber)bullismo, il nostro Istituto si avvale della collaborazione di enti che operano sul nostro territorio, nonché dell'Arma dei Carabinieri. Il referente coordina con le Forze dell'Ordine incontri nell'ambito della cultura alla legalità, volti a prevenire nei giovani studenti comportamenti scorretti che riguardano in particolare l'abuso delle tecnologie attraverso la presentazione dei reati e delle relative sanzioni. Si tengono contatti anche con i volontari provinciali di Telefono Azzurro e si realizzano attività di drammatizzazione con Noveteatro partendo dalle conoscenze dei ragazzi per arrivare a una riflessione condivisa del fenomeno, anche attraverso la realizzazione di un cortometraggio.

Tali incontri informativi e formativi sono rivolti anche ai genitori, essendo un momento di riflessione condiviso con la scuola, la psicologa scolastica, le forze dell'Ordine, l'amministrazione comunale e il parroco del nostro paese.

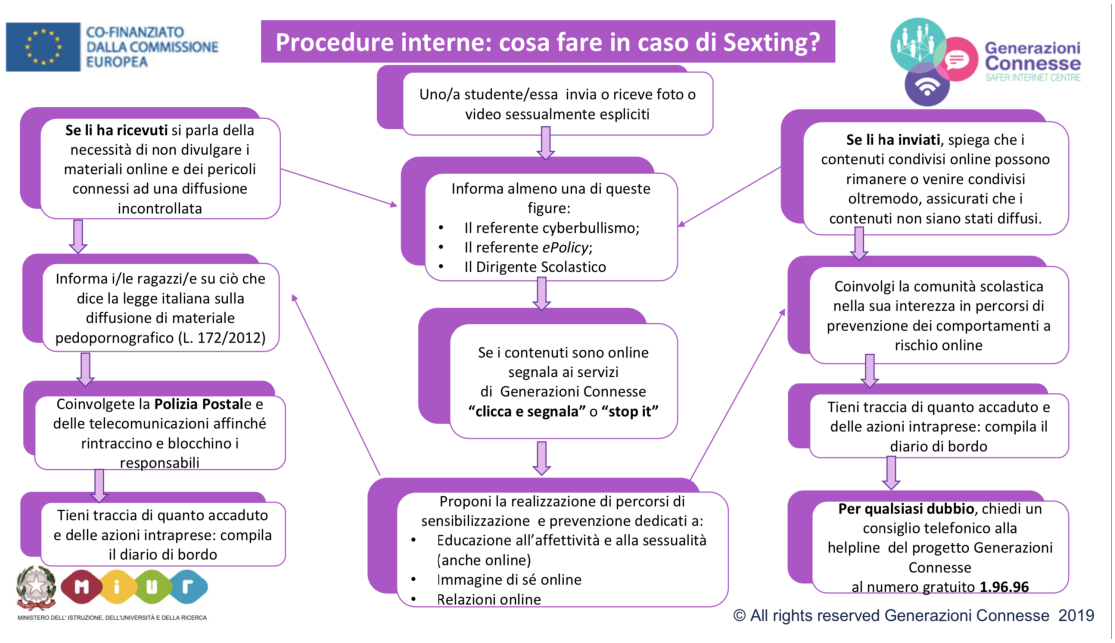
5.4. - Allegati con le procedure

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

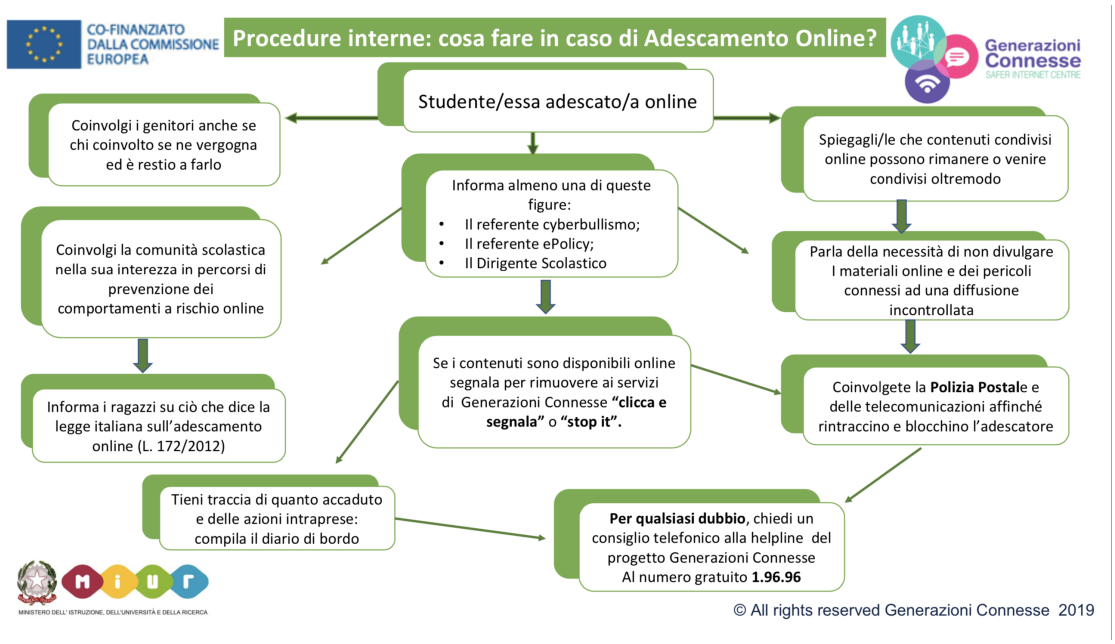




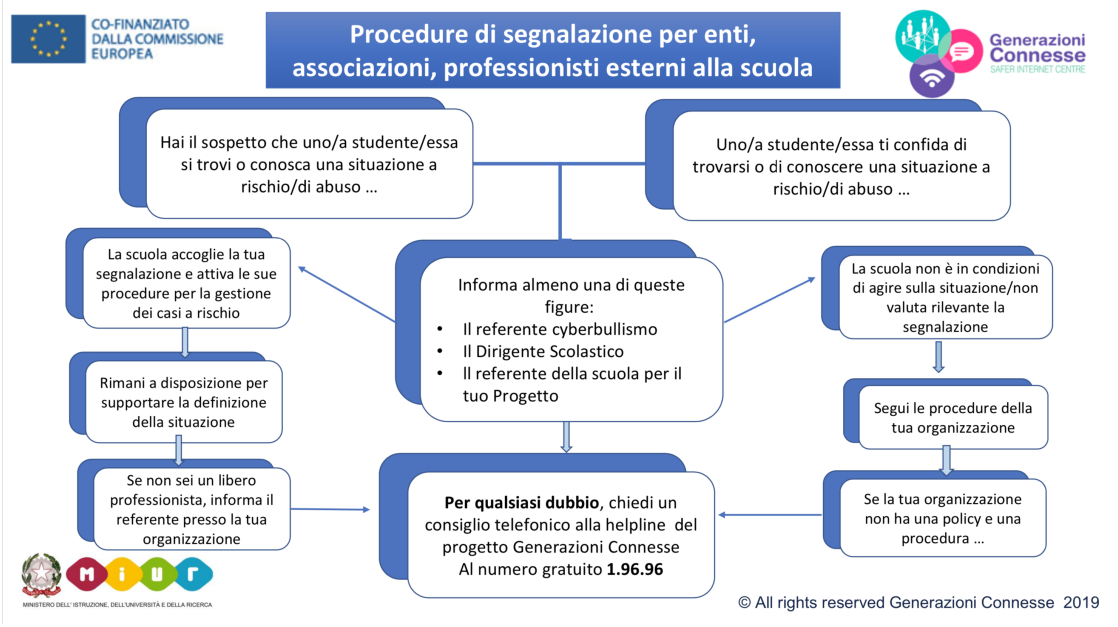
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



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



Altri allegati

- Scheda di segnalazione

- Diario di bordo
- iGloss@ 1.0 l'ABC dei comportamenti devianti online
- Elenco reati procedibili d'ufficio

Il nostro piano d'azioni

Il nostro Istituto continuerà a impegnarsi nella prevenzione e nel contrasto del (cyber)bullismo attraverso la realizzazione in tutte le classi della secondaria di primo grado di un percorso educativo e trasversale volto a diffondere un uso consapevole di Internet e dei Social Network.