ISTITUTO COMPRENSIVO "G. NASCIMBENI"
via G. Sinopoli, 38 - 37058 Sanguinetto (VR) C.F. 82001890233
Tel. 0442 81079 – 81031
e-mail: vric873005@istruzione.it - pec: vric873005@pec.istruzione.it
http://www.icsanguinetto.edu.it

Documento di ePolicy

VRIC873005

IC SANGUINETTO

VIA GIUSEPPE SINOPOLI 38 - 37058 - SANGUINETTO - VERONA (VR)

DIRIGENTE SCOLASTICO: CATERINA PAGANO

Argomenti del Documento

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 ePolicy, 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'ePolicy, 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'ePolicy 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.

Perché è importante dotarsi di una ePolicy?

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 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' ePolicy 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.

Lo scopo della ePolicy è di condividere e stabilire con tutti i membri della comunità scolastica regole, modalità e principi sull'utilizzo consapevole e corretto di internet.

In particolare essa viene redatta per regolare il comportamento della componente studentesca dentro le aule scolastiche e per sensibilizzarli all'adozione di buone pratiche quando sono fuori dalla scuola .

Il nostro Istituto accoglie minori "nativi digitali" che fin dalla scuola primaria sono esposti a rischi di cui sono inconsapevoli, pertanto la scuola si impegna ad attuare parallelamente attività di prevenzione, controllo , sensibilizzazione e formazione.

1.2 - Ruoli e responsabilità

Affinché l'ePolicy 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.

Nell'ambito di questa ePolicy sono individuati i seguenti ruoli e le principali responsabilità correlate:

I dirigenti scolastici sono chiamati a effettuare misure di intervento immediato qualora vengano a conoscenza di episodi di cyber bullismo. Tali misure dovranno essere integrate e previste nei Regolamenti di Istituto e nei Patti di Corresponsabilità.

Dirigente scolastico:

- garantisce la tutela degli aspetti legali riguardanti la privacy e la tutela dell'immagine di tutti i membri della comunità scolastica;
- garantisce ai propri docenti una formazione di base sulle tecnologie dell'Informazione e della Comunicazione (ICT) che consenta loro di possedere le competenze necessarie all'utilizzo di tali risorse;
- garantisce l'esistenza di un sistema che consenta il monitoraggio e il controllo interno della sicurezza on- line;
- informa tempestivamente, qualora venga a conoscenza di atti di cyberbullismo che non si configurino come reato, i genitori dei minori coinvolti; (o chi ne esercita la responsabilità genitoriale o i tutori);
- regola il comportamento degli studenti ed impone sanzioni disciplinari in caso di comportamento inadeguato.

Referente Cyberbullismo d'Istituto:

- Coordina iniziative di prevenzione e contrasto del cyberbullismo messe in atto dalla scuola;
- predispone un documento di rilevazione di incidenti di sicurezza in rete;
- facilita la formazione e la consulenza di tutto il personale.

Animatore digitale e Team dell'innovazione:

- Pubblicano il presente documento di E-Safery Policy sul sito della scuola;
- Diffondono i contenuti del documento tra docenti e studenti.

Insegnanti:

- provvedono personalmente alla propria formazione/aggiornamento sull'utilizzo del digitale con particolare riferimento alla dimensione etica (tutela della privacy, rispetto dei diritti intellettuali dei materiali reperiti in internet e dell'immagine degli altri: lotta al cyberbullismo);
- supportano gli alunni nell'utilizzo consapevole delle tecnologie informatiche utilizzate a scopi didattici;
- segnalano al Dirigente Scolastico e ai suoi collaboratori eventuali episodi di violazione delle norme di comportamento stabilite dalla scuola, avviando le procedure previste in caso di violazione;
- supportano ed indirizzano alunni coinvolti in problematiche legate alla rete.

Direttore dei Servizi Generali e Amministrativi:

- assicura, nei limiti delle risorse finanziarie disponibili, gli interventi di manutenzione necessari ad evitare un cattivo funzionamento della dotazione Tecnologica dell'Istituto, controllando al contempo che le norme di sicurezza vengano rispettate.

Genitori:

- contribuiscono, in sinergia con il personale scolastico, alla sensibilizzazione dei propri figli sul tema della sicurezza in rete;
- incoraggiano l'impiego delle ICT da parte degli alunni nello svolgimento dei compiti a casa, controllando che tale impiego avvenga in sicurezza;
- agiscono in modo concorde con la scuola per la prevenzione dei rischi e l'attuazione delle procedure previste in caso di violazione delle regole stabilite;
- rispondono per gli episodi commessi dai figli minori a titolo di culpa in educando (articolo 2048 del Codice Civile). Sono esonerati da responsabilità solo se dimostrano di non aver potuto impedire il fatto. Nei casi più gravi i giudici per l'inadeguatezza dell'educazione impartita ai figli emerge dagli stessi episodi di bullismo, che per le loro modalità esecutive dimostrano maturità ed educazione carenti.

Alunni:

- usano in modo responsabile, in relazione al proprio grado di maturità e di apprendimento, le tecnologie digitali in conformità con quanto richiesto dai docenti;
- avere una buona comprensione delle potenzialità offerte dalle TIC per la ricerca di contenuti e materiali ma anche della necessità di evitare il plagio e rispettare i diritti d'autore;
- comprendono l'importanza di adottare buone pratiche di sicurezza online quando si utilizzano le tecnologie digitali per non correre rischi;
- comprendono l'importanza di adottare buone pratiche di sicurezza online quando si usano le tecnologie digitali fuori dalla scuola.

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).

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

Il documento di ePolicy 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'ePolicy 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.

L'Istituto si impegna a diffondere la presente Policy per condividerne i contenuti con tutta la comunità scolastica.

La Policy sarà comunicata al personale, agli alunni, alla comunità nei seguenti modi:

- pubblicazione della ESafety Policy sul sito della scuola;

Successivamente si condividerà nelle seguente modalità a seconda degli attori interessati per raggiungere in modo più incisivo le singole parti:

a) La condivisione e comunicazione della la politica di e-safety agli alunni:

- istruire e informare gli alunni riguardo all'uso responsabile e sicuro di internet precederà l'accesso alla rete;
- sarà data particolare attenzione nell'educazione sulla sicurezza agli aspetti per i quali gli alunni risultano più esposti o rispetto ai quali risultano più vulnerabili.
- la scuola promuoverà quando possibile eventi e/o dibattiti informativi e formativi, in momenti diversi dell'anno, rivolti a tutto il personale, agli alunni e ai loro genitori, con il coinvolgimento di esperti, sui temi oggetto di codesto Documento.

Tra le misure di prevenzione che la scuola metterà in atto ci saranno, inoltre, azioni finalizzate a promuovere una cultura dell'inclusione, del rispetto dell'altro e delle differenze così che l'utilizzo di Internet e dei cellulari oltre che collocarci all'interno di un sistema di relazioni, ci renda consapevoli di gestire con un certo grado di trasparenza i rapporti che si sviluppano in tale ambiente, giungendo a riconoscere e gestire le proprie emozioni. A tal proposito si manterrà l'attivazione di uno "Sportello di ascolto" rivolto a tutti gli alunni, articolato in colloqui individuali e/o collettivi, al fine di migliorare il benessere personale e scolastico mediante un'attività di supporto della sfera emotiva, relazionale e comportamentale. Si prevede al suo interno, anche uno spazio riservato ai docenti e genitori al fine di individuare strategie efficaci per affrontare problematiche tipiche dell'età adolescenziale.

b) La condivisione e comunicazione della la politica di e-safety al personale:

- La linea di condotta della scuola in materia di sicurezza nell'utilizzo delle tecnologie digitali e di internet sarà discussa negli organi collegiali (consigli di interclasse/intersezione, collegio dei docenti) e comunicata formalmente a tutto il personale con il presente documento e altro materiale informativo anche sul sito web;
- Tutto il personale è consapevole che una condotta non in linea con il codice di comportamento dei pubblici dipendenti e i propri doveri professionali è sanzionabile.
- Sarà previsto un confronto collegiale, su base annuale, circa la necessità di apportare modifiche e miglioramenti alla policy vigente da parte del gruppo di lavoro ePolicy.

c) La condivisione e comunicazione della politica di e-safety ai genitori:

- l'attenzione dei genitori sulla sicurezza nell'uso delle tecnologie digitali e di internet sarà attirata attraverso il sito web della scuola;
- allo scopo di condividere regole comuni per l'utilizzo sicuro di Internet sia a casa che a scuola, si invitano tutti i genitori a prestare la massima attenzione ai principi e alle regole contenute nel presente documento.

1.5 - Gestione delle infrazioni alla ePolicy

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

- Richiamo verbale;
- Sanzioni estemporanee commisurate alla gravità della violazione commessa (assegnazione di attività aggiuntive da svolgere a casa sui temi di Cittadinanza e Costituzione);
- Nota informativa ai genitori o 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 bullismo On-line saranno trattate in conformità con la legge.

1.6. - Integrazione dell'ePolicy con Regolamenti esistenti

Il Regolamento dell'Istituto Scolastico viene aggiornato con specifici riferimenti all'ePolicy, 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 ePolicy safety o regolamento per l'uso delle risorse tecnologiche e di rete è stato allegato al Regolamento di Istituto e inserito nel sito web della scuola.

I genitori vengono informati della pubblicazione del presente "Regolamento per l'uso delle risorse tecnologiche e di rete" della scuola e possono prenderne visione sul sito della scuola.

1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

L'ePolicy 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 nostro piano d'azioni

AZIONI da svolgere entro un'annualità scolastica

- Organizzare uno o più eventi o attività svolti a presentare il progetto e consulta dell'Istituto per la stesura finale delle policy

AZIONI da svolgere nei prossimi tre anni

- Organizzare un evento di presentazione del progetto generazioni connesse rivolto agli studenti.
- Organizzare un evento di presentazione del progetto generazioni connesse rivolto ai docenti.

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.

Nell'ambito del PNSD questa scuola si propone un programma di progressiva educazione alla sicurezza, online come parte del curriculum scolastico. Si impegna a sviluppare una serie di competenze e comportamenti adeguati alle età degli alunni e ad esperienza, tra cui:

- programmare attività e far partecipare gli alunni a laboratori di utilizzo consapevole e appropriato delle Tic;
- conoscere le conseguenze disciplinari della scuola, civili e penali in caso di denuncia e riscontro oggettivo di infrazioni inerente un utilizzo scorretto degli smartphone e contrario alla presentePolicy o al regolamento di istituto;
- capire il motivo per cui non devono pubblicare foto o video di altri senza il loro permesso;
- capire il motivo per cui qualsiasi materiale scritto, pubblicato e postato sui social è sempre tracciabile e può rimanere per sempre;
- capire che condividere è essere ugualmente responsabili di ciò che vi è all'interno del gruppo;
- capire perché 'amici' on-line potrebbero non essere chi dicono di essere e di comprendere perché dovrebbero fare attenzione in un ambiente online;
- comprendere l'impatto di bullismo online, sexting, grooming e sapere come cercare aiuto se sono in pericolo;
- sapere come segnalare eventuali abusi tra cui il bullismo on-line e come chiedere aiuto ai docenti, ai genitori, se si verificano problemi quando si utilizzano le tecnologie Internet;
- utilizzare con attenzione Internet per garantire che si adatti alla loro età e supporti gli obiettivi di apprendimento per le aree curriculari specifiche;
- sviluppare una serie di strategie per valutare e verificare le informazioni prima di accettarne l'esattezza;
- sapere come restringere o affinare una ricerca

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.

La formazione del corpo docente, intesa come processo permanente, deve prevedere:

- momenti di auto-aggiornamento;
- formazione specifica, con apporto di docenti preparati, o organizzando conferenze tenute da esperti esterni, per permettere un'adeguata formazione agli insegnanti sull'uso e l'inserimento delle TIC nella didattica e ai temi informatici in generale;
- informazione su corsi, convegni e seminari che riguardino tali argomenti, cercando altresì di agevolare il personale che intenda parteciparvi;
- adesione a progetti appositi di formazione, presentati da enti e associazioni, come già avvenuto in passato.

2.3 - Formazione dei docentisull'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 in ingresso e in servizio è senza dubbio il cardine per assicurare l'adeguatezza della professionalità docente ai bisogni formativi ed educativi degli studenti. Prioritario, infatti, appare il coinvolgimento degli insegnanti ai quali vanno rivolti moduli di formazione che rafforzino le competenze necessarie a individuare tempestivamente eventuali risvolti psicologici conseguenti all'uso distorto delle nuove tecnologie e alla violenza in contesti faccia a faccia. La scuola partecipa dal 2018/19 al programma "generazioni connesse" sui cui è disponibile una piattaforma di formazione destinata a tutti i docenti dell'Istituto che vogliano formarsi sull'argomento specifico delle nuove tecnologie.

Quest'anno l'istituto si è impegnato a redigere un nuovo documento ePolicy, aggiornando il testo già presente.

2.4 - Sensibilizzazione delle famiglie e integrazioni al Patto di Corresponsabilità

Nella prevenzione dei rischi connessi ad un uso non consapevole delle TIC, così come nella promozione di un loro uso positivo e capace di coglierne le opportunità, è necessaria la collaborazione di tutti gli attori educanti, ognuno secondo i propri ruoli e le proprie responsabilità. Scuola e famiglia devono rinforzare l'alleanza educativa e

promuovere percorsi educativi continuativi e condivisi per accompagnare insieme ragazzi/e e bambini/e verso un uso responsabile e arricchente delle tecnologie digitali, anche in una prospettiva lavorativa futura. L'Istituto garantisce la massima informazione alle famiglie di tutte le attività e iniziative intraprese sul tema delle tecnologie digitali, previste dall'ePolicy e dal suo piano di azioni, anche attraverso l'aggiornamento, oltre che del regolamento scolastico, anche del "Patto di corresponsabilità" e attraverso una sezione dedicata sul sito web dell'Istituto.

La scuola avrà continua cura di sensibilizzare le famiglie, specificandone l'importanza anche nel Patto Educativo di Corresponsabilità, attraverso documentazione informativa, ad un corretto uso delle nuove tecnologie da parte dei ragazzi a casa e a scuola, indicando, anche alcune semplici azioni che possono rendere la navigazione sicura.

In modo particolare:

- far conoscere , condividere e presentare ai genitori il Regolamento della Policy, al fine di garantire che i principi di comportamento sicuro on-line siano chiari;
- fornire informazioni sui siti nazionali di sostegno per i genitori, quali il sito www.generazioniconnesse.it.

Il nostro piano d'azioni

AZIONI da svolgere entro un'annualità scolastica

- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.

AZIONI da svolgere nei prossimi tre anni

- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali

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

3.1 - Protezione dei dati personali

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

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

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

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

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

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

Il personale scolastico, accuratamente informato, è "incaricato del trattamento" dei dati personali (degli alunni, dei genitori, ecc.), nei limiti delle operazioni di trattamento e delle categorie di dati necessarie ai fini dello svolgimento della propria funzione e nello specifico della docenza (istruzione e formazione).

Viene inoltre fornita ai genitori informativa e richiesta di autorizzazione all'utilizzo dei dati personali degli alunni riguardante i trattamenti istituzionali obbligatori.

La scuola metterà in atto tutte le azioni necessarie per garantire agli studenti l'accesso alla documentazione cercata adottando tutti i sistemi di sicurezza conosciuti per diminuire le possibilità di rischio durante la navigazione.

Resta fermo che non è possibile garantire una navigazione totalmente priva di rischi e che la Scuola e gli insegnanti non possono assumersi le responsabilità conseguenti all'accesso

accidentale e/o improprio a siti illeciti.

Linee guida di buona condotta dell'utente e buone pratiche nell'uso della rete

- rispettare la legislazione vigente;
- tutelare la propria privacy, quella degli altri utenti e degli alunni al fine di non divulgare notizie private contenute nelle documentazioni elettroniche cui hai accesso;
- rispettare la cosiddetta netiquette (regole condivise che disciplinano il rapportarsi fra utenti della rete, siti, forum, mail e di qualsiasi altro tipo di comunicazione).
- rispetto dei diritti di autore e dei diritti di proprietà intellettuale.

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.

1. L'accesso a Internet, possibile in tutti i plessi, nei laboratori di informatica e in quasi tutte le aule, è consentito al personale docente e non docente solo ad esclusivo uso didattico e/o di formazione e alle classi accompagnate e sotto la responsabilità di un insegnante;

2. Internet non può essere usato per scopi vietati dalla legislazione vigente;
3. L'utente è direttamente responsabile, civilmente e penalmente, a norma delle vigenti leggi, per l'uso fatto del servizio Internet;
4. È vietato inserire sui pc connessi in rete programmi contenenti virus, scaricare software non autorizzati da internet, scaricare e installare software senza licenza. Le impostazioni sono definite e manutenute dall'Animatore digitale ed è in carico a ciascun docente la segnalazione di malfunzionamenti e disservizi. Consultare obbligatoriamente prima di installare qualsiasi programma, l'animatore digitale, un responsabile di laboratorio o un tecnico per valutarne la compatibilità.

Relativamente agli alunni che accedono a Internet durante l'attività didattica sono consentiti la navigazione guidata da parte dell'insegnante e la stesura di documenti collaborativi purché sotto il controllo dell'insegnante e nel caso in cui tale attività faccia parte di un progetto di lavoro precedentemente autorizzato.

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.

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

Le comunicazioni tra personale scolastico, famiglie e allieve/allievi devono avvenire preferibilmente tramite registro elettronico. E-mail in arrivo da mittenti sconosciuti vanno trattate come sospette ed eventuali allegati non devono essere aperti.

Il Dirigente Scolastico e il personale incaricato di gestire le pagine del sito della Scuola hanno la responsabilità di garantire che il contenuto pubblicato sia accurato e appropriato. La scuola offre all'interno del proprio sito una serie di servizi alle famiglie e ai fruitori esterni: i docenti che desiderano pubblicare attività didattiche dovranno chiedere l'autorizzazione al Dirigente.

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.

- Gli studenti non possono utilizzare i propri dispositivi durante le attività didattiche né possono accedere alla rete attraverso i dispositivi della scuola se non con autorizzazione dell'insegnante presente in aula e comunque per ricerche attinenti le attività didattiche.
- Studenti con disturbi specifici di apprendimento o altre disabilità certificate, previa consultazione con il Consiglio di Classe, concorderanno le modalità di impiego di strumenti compensativi quali tablet e computer portatili e le modalità di custodia.
- Nel caso in cui debbano comunicare con la famiglia durante l'orario scolastico, alunne e alunni possono usare gratuitamente la linea fissa della scuola rivolgendosi a un operatore; allo stesso modo le famiglie devono chiamare il centralino della scuola se hanno assoluta necessità di parlare con i propri figli. Si raccomanda di ridurre tali comunicazioni a casi di inderogabile necessità e urgenza.
- L'Istituzione Scolastica non ha e comunque non si assume alcuna responsabilità né relativamente all'uso improprio o pericoloso che gli studenti dovessero fare del cellulare, né relativamente a smarrimenti e/o 'sparizioni' di telefonini cellulari o di hard/disk portatili o pen-drive.
- Durante le ore di lezione è consentito ai docenti l'uso di dispositivi elettronici personali, come il tablet, unicamente a scopo didattico e a integrazione dei dispositivi scolastici disponibili (il computer di classe), in special modo per l'utilizzo del registro elettronico. Durante il restante orario di servizio l'uso del cellulare è consentito solo per comunicazioni personali che rivestano carattere di urgenza, mentre l'uso di altri dispositivi elettronici personali è permesso per attività funzionali all'insegnamento.
- Durante l'orario di servizio al restante personale scolastico l'uso del cellulare è consentito per comunicazioni personali urgenti. L'uso di altri dispositivi elettronici personali è permesso solo per attività funzionali al servizio, e preventivamente autorizzato.

Il nostro piano d'azioni

AZIONI da svolgere nei prossimi tre anni

- 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 una 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.

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

4.1 - Sensibilizzazione e prevenzione

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

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

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

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

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

La Scuola ha scelto di creare un ambiente di apprendimento sereno e sicuro in cui sia chiaro sin dal primo giorno di scuola che (cyber)bullismo, prepotenza, aggressione e violenza non sono permessi, in cui ci sia l'apertura necessaria all'incoraggiamento a parlare di sé e dei propri problemi, che stimoli alla partecipazione diffusa di tutta la comunità scolastica nelle azioni finalizzate al contrasto del (cyber)bullismo, che insegni ad interagire in maniera responsabile.

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).

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.

L'Istituto, pur non dedicando attività specifiche alla prevenzione dell'hate speech, favorisce in ogni momento la costruzione di una modalità d'intervento non ostile e non basata su stereotipi offensivi e non fondati. Ogni docente, all'interno delle sue discipline e delle sue ore con gli studenti e le studentesse, dedica tempo ed energie alla costruzione di un ascolto attivo e di un dialogo pacifico. La partecipazione civica e l'impegno dei ragazzi, inoltre, sono promossi da progetti (come CCR) costruiti in collaborazione con le Amministrazioni comunali grazie ai quali gli studenti e le studentesse conoscono in maniera diretta ed esperienzale i processi democratici con la mediazione e l'aiuto di esperti del settore.

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.

Se si ha il sospetto che un minore possa essere stato colpito da questo tipo di patologia, il primo strumento nelle mani dell'adulto, insegnante o genitore, di riferimento è quello di mantenere un dialogo aperto con il bambino o ragazzo.

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.

La questione delle relazioni affettive e della sessualità è sempre stata di primaria importanza per chiunque sia in relazione con ragazzi adolescenti ma oggi la pervasività della tecnologia digitale è riuscita a rendere il tema ancora più pressante e delicato.

Il termine ***sexting***, è un neologismo creato dalla crasi delle parole inglesi *sex* (sesso) e *texting* (inviare SMS), utilizzato per indicare l'invio di messaggi o immagini sessualmente espliciti utilizzando smartphone ed altri strumenti informatici.

Le relazioni affettive e sessuali tra gli adolescenti di questi tempi comprendono anche lo scambio di diversi contenuti attraverso i dispositivi e i social network. Quei contenuti possono anche essere immagini, video o messaggi sessualmente espliciti che sono inviati, ricevuti o inoltrati online.

I problemi sorgono quando i messaggi e le immagini a contenuto sessuale vengono condivisi senza autorizzazione. Può essere in questo caso considerato come una pesante prevaricazione, tanto quanto il cyberbullismo, con un alto e identico livello di pericolosità per il benessere mentale.

Sarà importante, nei momenti di discussione, di approfondimento, di confronto, lasciare liberi i bambini e i ragazzi, di parlare, di condividere, di farli sentire capiti, anche se a volte è complicato.

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).

La scuola, attraverso la realizzazione di percorsi didattici , si pone l'obiettivo di sensibilizzare gli studenti sui rischi di un'amicizia "in 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.

Il nostro piano d'azioni

AZIONI da svolgere nei prossimi tre anni

- Organizzare uno o più incontri di sensibilizzazione sui rischi on-line e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli/lle studenti/studentesse.
- Organizzare uno o più incontri per la promozione del rispetto delle diversità: rispetto delle differenze di genere, di orientamento e identità sessuale, di cultura e provenienza, eccetera, con la partecipazione attiva degli/lle studenti/studentesse

Capitolo 5 - Segnalazione e gestione deicasi

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 comunitàscolastica.

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 (come da allegati).

Tali procedure dovranno essere una guida costante per il personale della scuola nell'identificazione di una situazione online a rischio, così da definire le modalità di presa in carico da parte della scuola e l'intervento migliore da mettere in atto per aiutare studenti/esse in difficoltà. Esse, inoltre, forniscono valide indicazioni anche per i professionisti e le organizzazioni esterne che operano con la scuola (vedi paragrafo 1.3. dell'ePolicy).

Nelle procedure:

- sono indicate le **figure preposte all'accoglienza della segnalazione e alla presa in carico e gestione del caso**.
- le modalità di coinvolgimento del referente per il contrasto del bullismo e del cyberbullismo, oltre al Dirigente Scolastico.
- Inoltre, la scuola **individua le figure che costituiranno un team** preposto alla gestione della segnalazione (gestione interna alla scuola, invio ai soggetti competenti).

Nell'affrontare i casi prevediamo la **collaborazione con altre figure, enti, istituzioni e servizi presenti sul territorio** (che verranno richiamati più avanti), qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.

Tali procedure sono comunicate e condivise con l'intera comunità scolastica.

Questo risulta importante sia per facilitare l'emersione di situazioni a rischio, e la conseguente presa in carico e gestione, sia per dare un messaggio chiaro a studenti e studentesse, alle famiglie e a tutti coloro che vivono la scuola che la stessa è un luogo sicuro, attento al benessere di chi lo vive, in cui le problematiche non vengono ignorate ma gestite con una mobilitazione attenta di tutta la comunità.

La condivisione avverrà attraverso assemblee scolastiche che coinvolgono i genitori, gli studenti e le studentesse e il personale della scuola, con l'utilizzo di locandine da affiggere a scuola, attraverso news nel sito della scuola e durante i collegi docenti e attraverso tutti i canali maggiormente utili ad un'efficace comunicazione.

A seguire, le problematiche a cui fanno riferimento le procedure allegate:

- **Cyberbullismo**: è necessario capire se si tratta effettivamente di cyberbullismo o di altra problematica. Oltre al contesto, vanno considerate le modalità attraverso le quali il comportamento si manifesta (alla presenza di un "pubblico"? Tra coetanei? In modo ripetuto e intenzionale? C'è un danno percepito alla vittima? etc.). È necessario poi valutare l'eventuale stato di disagio vissuto dagli/lle studenti/esse coinvolti/e (e quindi valutare se rivolgersi ad un servizio deputato ad offrire un

supporto psicologico e/o di mediazione).

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

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

Vi suggeriamo, inoltre, i seguenti servizi:

- Servizio di Helpline 19696 e Chat di Telefono Azzurro per supporto ed emergenze;
- Clicca e segnala di Telefono Azzurro e STOP-IT di Save the Children Italia per segnalare la presenza di materiale pedopornografico online.

5.2 - Come segnalare: quali strumenti e a chi

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

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

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

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

Per tutti i dettagli consultare gli 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 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 19696.

Il Team e il consiglio di Classe, dopo essere stati allertati da un genitore, un alunno o da uno dei componenti della comunità scolastica, contattano prontamente il Dirigente Scolastico per comunicargli l'accaduto e d'accordo con la dirigenza vengono stabiliti tempi e modi di comunicazione alla famiglia e i successivi passi da intraprendere. Nel caso in cui un docente sospetti che stia avvenendo qualcosa riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online fra gli studenti e le studentesse, informa i colleghi titolari sulla classe osservano e monitorano il clima di classe e le dinamiche relazionali. Nel caso in cui un docente abbia certezza del fatto che siano avvenuti casi riferibili a bullismo e/o cyberbullismo, sexting o adescamento online, invece, viene avvisato il Dirigente Scolastico che può convocare il Consiglio di Classe e, in base alla gravità della situazione, stabilisce in che tempi e con che modalità avvisare le famiglie degli studenti e delle studentesse direttamente coinvolti. A seconda della situazione e delle valutazioni effettuate, il caso può essere segnalato alle autorità competenti e si può richiedere, se ritenuto opportuno, il sostegno dei servizi e delle associazioni territoriali.

Il personale della scuola, anche con l'ausilio del personale di assistenza tecnica, dovrà provvedere a:

1. conservare le eventuali tracce di una navigazione non consentita su internet o del passaggio di materiali inidonei sui pc della scuola;
2. tempestiva informazione delle famiglie in merito all'accaduto, anche per consentire ulteriori indagini e, in assenza di prove oggettive, di raccogliere testimonianze sui fatti da riferire al Dirigente Scolastico e, eventualmente, alla Polizia Postale.

Per i reati più gravi la scuola si rivolgerà direttamente agli organi e alle agenzie deputati alla presa in carico dei vari aspetti che una problematica connessa all'utilizzo di internet può presentare.

Gli strumenti per segnalare e monitorare i casi a scuola sono due:

1. nell'effettuare la segnalazione seguire ed utilizzare il " modulo apposito di segnalazione" ALLEGATO 1 affinché le segnalazioni vengano effettuate per iscritto e contengano tutte le informazioni necessarie alla presa in carico della situazione.
2. utilizzare poi l'ALLEGATO 2 – "Diario di bordo " per tenere traccia di ciò che è avvenuto rispetto ai comportamenti degli alunni online e di come è stato gestito.

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.

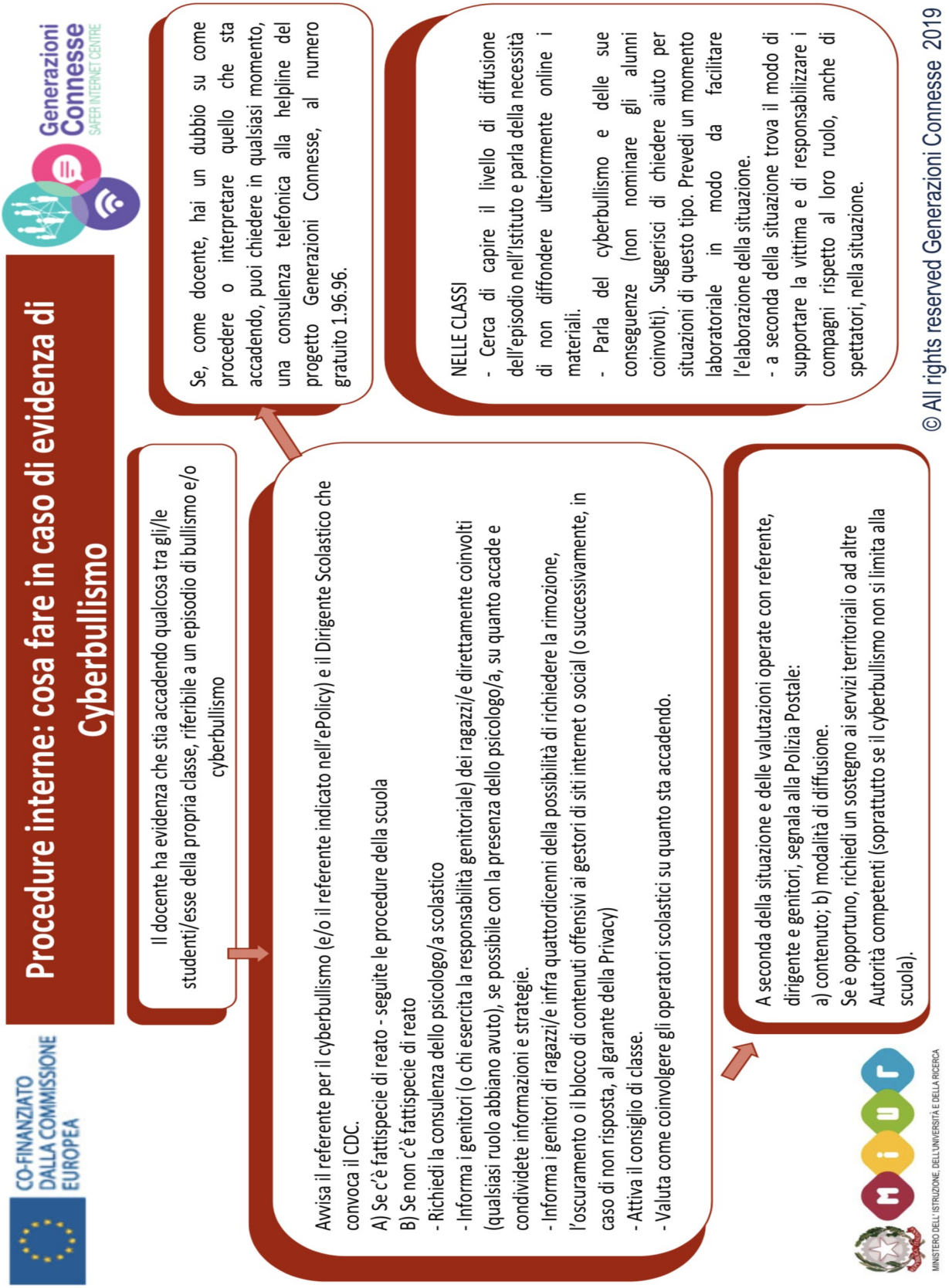
- **Comitato Regionale Unicef**: laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni)**: svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare 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.
- UFFICIO POLIZIA COMUNE DI SANGUINETTO E GAZZO VERONESE

  boarati@comune.sanguinetto.vr.it

  polizialocale@comune.gazzo.vr.it
- Servizi sociali comunali e di Ambito
- Agenzie educative del territorio
- I due servizi messi a disposizione dal Safer Internet Center sono:
  - Clicca e segnala di Telefono Azzurro www.azzurro.it/it/clicca-e-segnala
  - Stop-it di Save the Children www.stop-it.it

5.4 - Allegati con le procedure

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



CO-FINANZIATO DALLA COMMISSIONE EUROPEA

Procedure interne: cosa fare in caso di sospetto di Cyberbullismo

Generazioni Connesse
SAFER INTERNET CENTRE

Il docente sospetta che stia accadendo qualcosa tra gli studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo

Sonda il clima di classe, ascoltando i ragazzi e monitorando ciò che accade (ma senza fare indagini o interrogatori).
Cerca di capire il livello di diffusione dell'episodio a livello di Istituto.

Condividi con il referente per il cyberbullismo (e/o il referente indicato nell'e-policy): valuta con lui/loro le possibili strategie di intervento.

Valuta se è il caso di avvisare il consiglio di classe.
Valuta se è il caso di avvisare il Dirigente Scolastico, anche in base al regolamento interno o a prassi consolidate.

Se, come docente, hai un dubbio su come procedere o interpretare quello che sta accadendo, puoi chiedere in qualsiasi momento, una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

Parla in classe del cyberbullismo e delle sue conseguenze (non nominare gli alunni che sospetti coinvolti). Suggerisci di **chiedere aiuto** per situazioni di questo tipo.
Proponi attività in classe sull'empatia e sul riconoscimento delle emozioni (proprie e altrui)

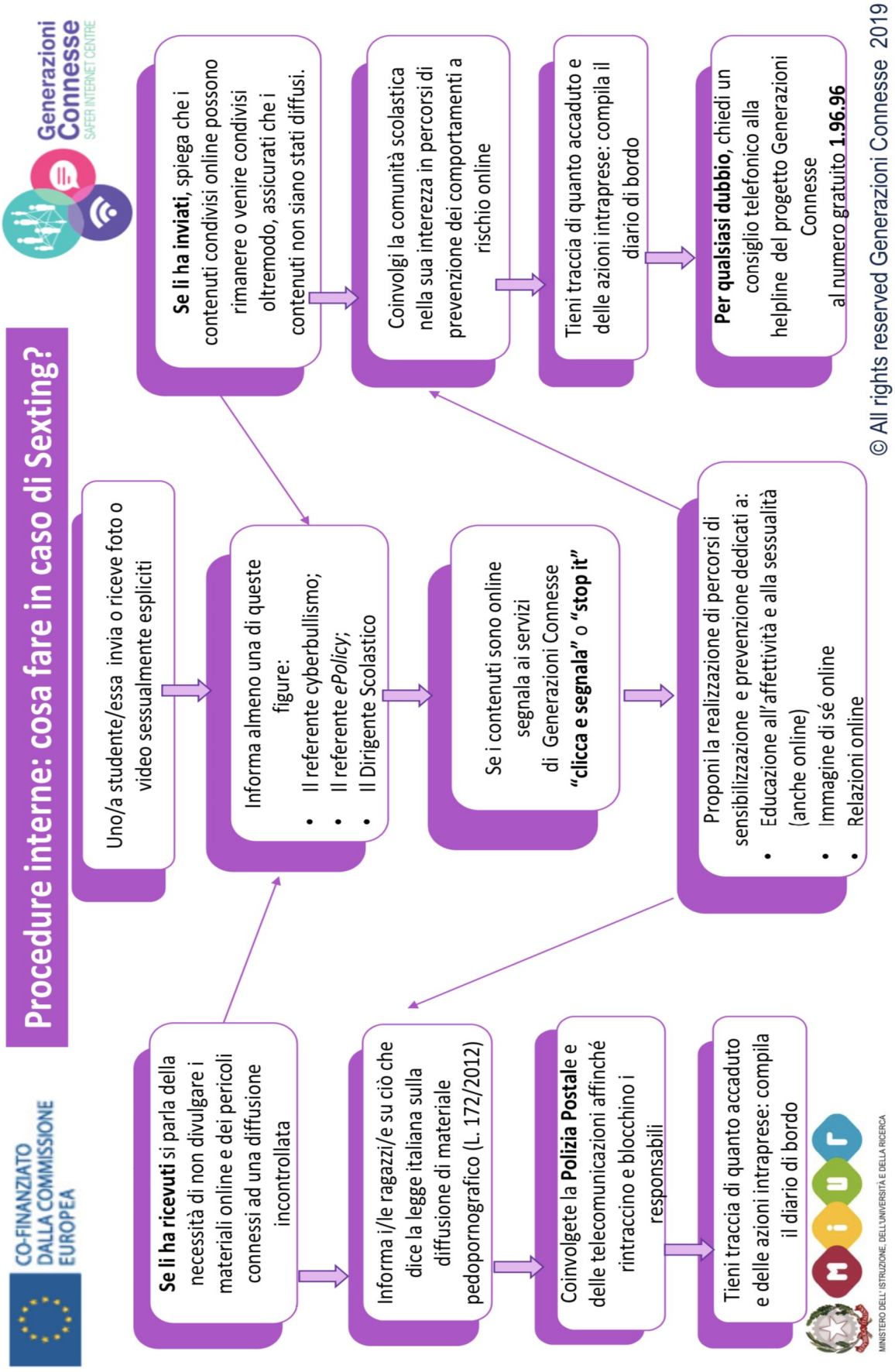
Se emergono evidenze passa allo schema successivo

Informa i/le ragazzi/e su ciò che dice la legge italiana su cyberbullismo L. 71/2017)
Ricorda agli studenti che possono segnalare al gestore del sito/social e al garante privacy eventuali contenuti offensivi/lesivi che li riguardano

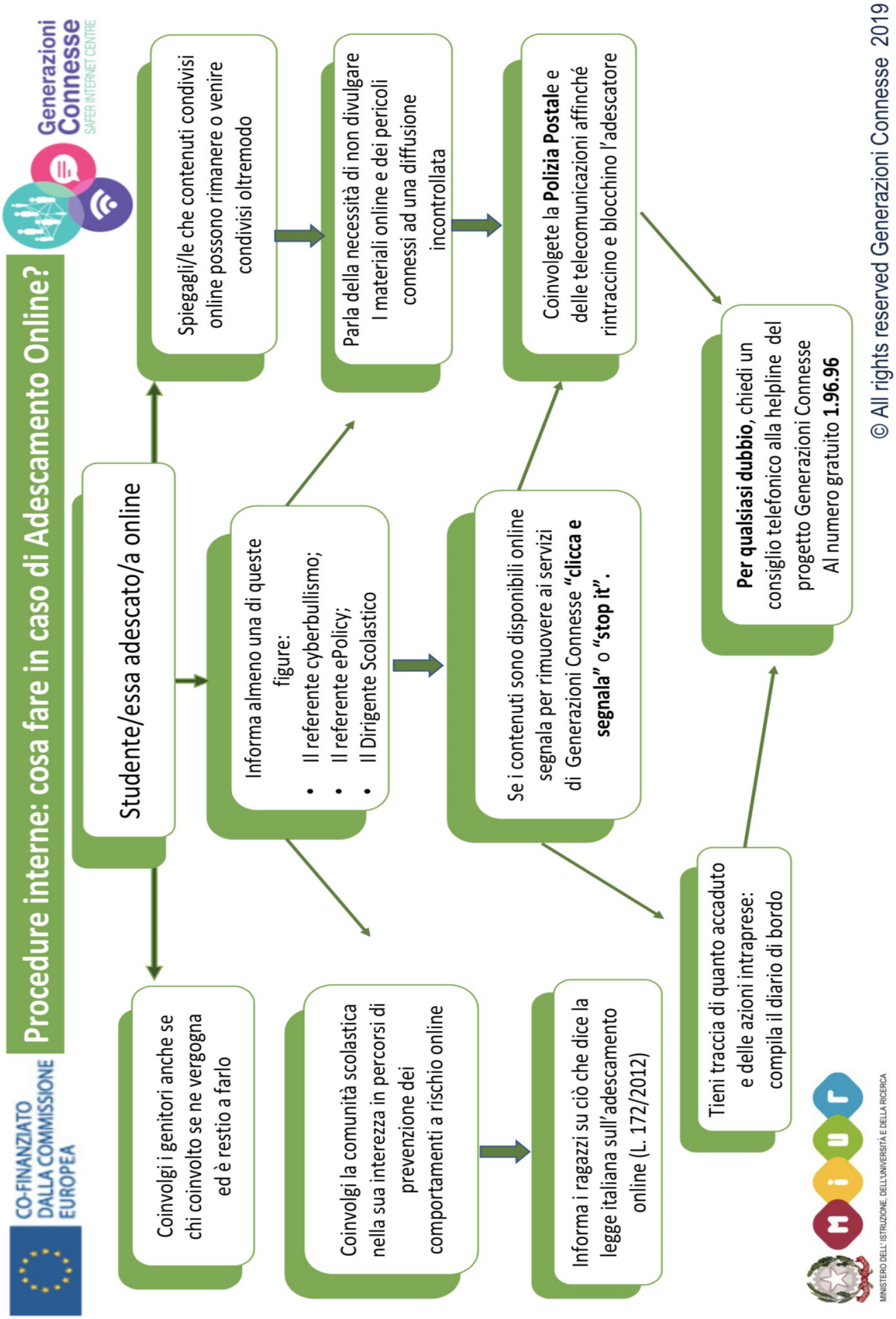
Ricorda a studenti/esse che possono chiedere in qualsiasi momento una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96 o via chat

MINISTERO DELL' ISTRUZIONE, DELL'UNIVERSITÀ E DELLA RICERCA

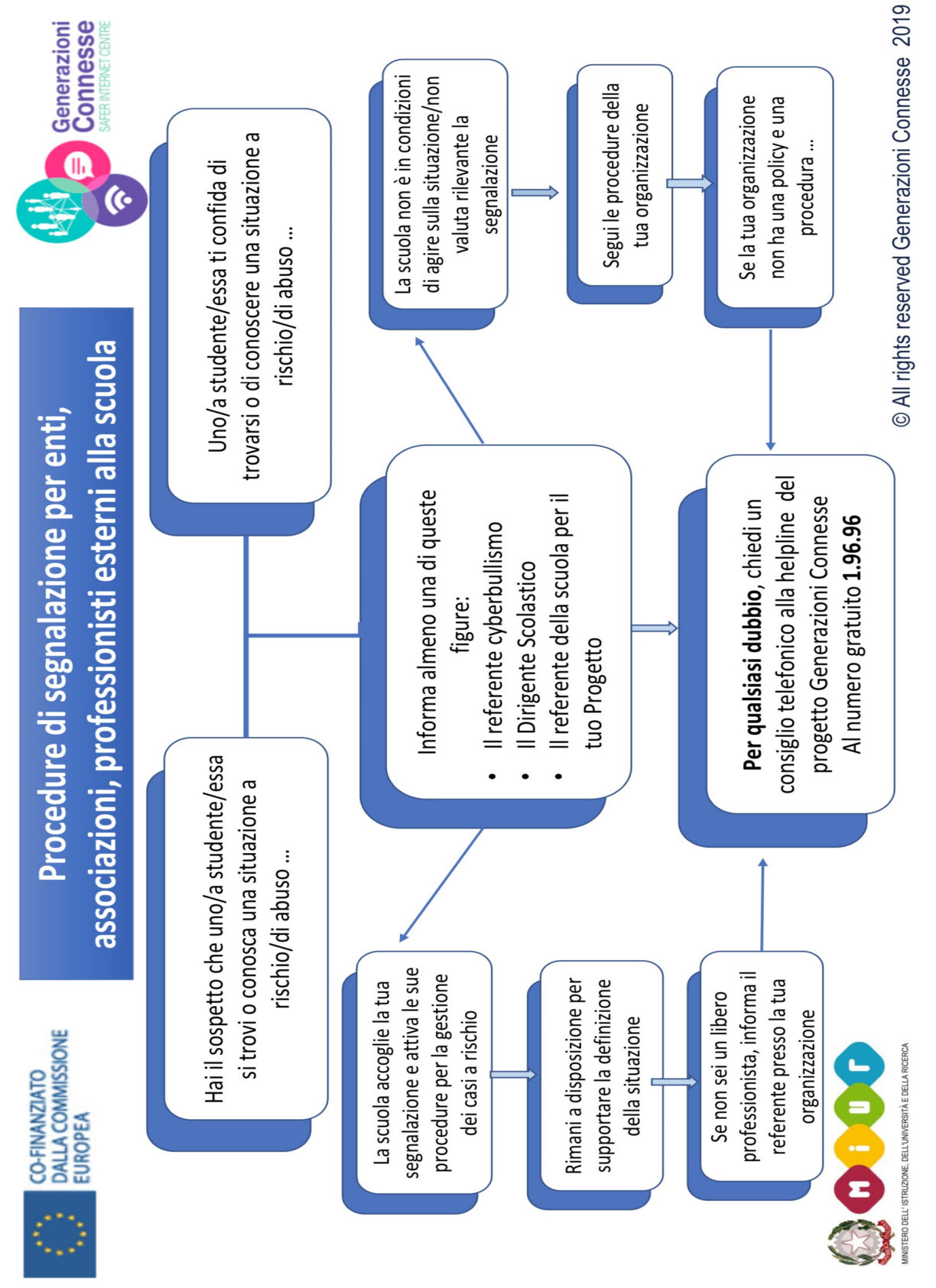
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



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



Altri allegati

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

Il nostro piano d'azioni

Non è prevista nessuna azione