Documento di ePolicy

LEIC85600E

I.C. "A. DIAZ"

VIA DELLA REPUBBLICAN.7 - 73029 - VERNOLE - LECCE (LE)

Pantaleo Antonio Conte

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.

  La scuola elabora il presente documento E-POLICY seguendo le indicazioni delle LINEE DI ORIENTAMENTO per azioni di prevenzione e di contrasto al bullismo e cyberbullismo elaborate dal Ministero dell'Istruzione, dell' Università e della Ricerca in collaborazione con Generazioni Connesse e il Safe Internet Center per l'Italia, programma comunitario istituito dal DF Europeo e dal consiglio dell'Unione.

  L'obiettivo è educare e sensibilizzare gli adolescenti, gli insegnanti e i genitori all'uso sicuro e consapevole di Internet.

  Il curricolo scolastico prevede che gli studenti imparino utilizzando le TIC e la scuola propone agli studenti e agli insegnanti di utilizzare internet per promuovere l'apprendimento in ambito didattico, attraverso la condivisione delle risorse, l'innovazione e la comunicazione.

  Gli insegnanti hanno la responsabilità di guidare gli studenti nell'attività online, di stabilire contatti chiari per un uso responsabile di internet.

Negli ultimi anni, la scuola ha cercato di dotarsi di strumenti tecnologici e di favorire la formazione del personale per far crescere le competenze professionali specifiche nell'impiego delle nuove tecnologie.

A tal fine, è stato formulato un regolamento per l'utilizzo e il corretto funzionamento delle aule e delle postazioni informatiche , tramite l'indicazione di pratiche opportune e l'invito ad un uso responsabile da parte di tutto il personale.

Scopo del presente documento di E-policy è di informare l'utenza per un uso corretto e responsabile delle apparecchiature informatiche, collegate alla rete in dotazione alla Scuola, nel rispetto della normativa vigente.

In particolare, l'intento della scuola è quello di promuovere l'uso consapevole e critico da parte degli alunni delle tecnologie digitali e di internet, di far acquisire loro procedure e competenze "tecniche", ma anche corrette norme comportamentali; di prevenire, ovvero rilevare e fronteggiare, le problematiche che derivano da un utilizzo non responsabile, pericoloso o dannoso, delle tecnologie digitali .

Gli utenti, soprattutto minori, devono essere pienamente consapevoli dei rischi a cui si espongono quando navigano in rete. Di fatto esiste la possibilità che durante il lavoro online si possa entrare accidentalmente in contatto con materiale inadeguato e/o illegale, pertanto la Scuola promuove l'adozione di strategie che limitino l'accesso a siti e/o applicazioni illeciti.

Argomenti del Documento

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.

Lo scopo della E-Policy è di stabilire i principi fondamentali per l'uso corretto e responsabile delle apparecchiature informatiche collegate alla rete in dotazione alla Scuola, seguendo le indicazioni di **Educazione Civica** riguardanti la **Cittadinanza Digitale,** emanate dal Miur. Inoltre, bisogna salvaguardare e proteggere i bambini, i ragazzi e il personale dell'Istituto con la promozione dell'uso consapevole e critico, delle tecnologie digitali e di internet, anche attraverso la conoscenza di corrette norme comportamentali (Netiquette), per prevenire e fronteggiare le problematiche che derivano da un utilizzo non responsabile, delle tecnologie digitali (Cyberbullismo).

1.2 - Ruoli e responsabilità

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

Ogni utente connesso alla rete deve:

1. rispettare il presente regolamento e la normativa vigente;
2. tutelare la propria privacy, quella degli altri adulti e quella degli studenti;
3. rispettare la "netiquette".

Dirigente Scolastico

Il ruolo del Dirigente scolastico nel promuovere l'uso consentito delle tecnologie e di internet include i seguenti compiti:

- responsabilità generale per i dati e la sicurezza dei dati;
- garantire che la scuola utilizzi un Internet Service approvato e conforme ai requisiti di legge vigenti;
- la responsabilità di assicurare che il personale riceva una formazione adeguata per svolgere i ruoli di sicurezza on-line;
- essere a conoscenza delle procedure da seguire in caso di infrazione dell e norme;
- ruolo di primo piano nello stabilire e rivedere il documento di E-Policy;

Direttore dei Servizi Generali e Amministrativi

Il ruolo del direttore dei servizi generali e amministrativi include i seguenti compiti:

- assicurare, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per garantire che l'infrastruttura tecnica della scuola sia funzionante, sicura e non aperta a dannosi attacchi esterni;
- garantire il funzionamento dei diversi canali di comunicazione della scuola (sportello, circolari, sito web) all'interno della scuola e fra la scuola e le famiglie degli alunni, per la notifica di documenti e informazioni riguardanti l'utilizzo delle tecnologie digitali e di internet.

Animatore digitale

Il ruolo dell'Animatore Digitale include i seguenti compiti:

- stimolare la formazione interna all'istituzione negli ambiti di sviluppo della "scuola digitale" e fornire consulenza e informazioni al personale, in relazione ai rischi on-line e alle misure di prevenzione e gestione degli stessi;
- monitorare e rilevare le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola;
- assicurare che gli utenti possano accedere alla rete della scuola solo tramite account istituzionali, generati dalla scuola;
- coinvolgere la comunità scolastica nella partecipazione ad attività e progetti attinenti la "scuola digitale"

Team digitale

Il ruolo del Team digitale include i seguenti compiti:

- pubblicare e diffondere il documento di E-Policy sul sito della scuola;
- monitorare e rilevare le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola;
- coinvolgere la comunità scolastica nella partecipazione ad attività e progetti attinenti la "scuola digitale";
- sviluppore il sito web della scuola per scopi istituzionali e consentiti

Docenti

I Docenti hanno la responsabilità di:

- illustrare agli studenti il presente documento;
- dare indicazioni sul corretto uso della rete;
- supervisionare e guidare gli alunni con cura quando sono impegnati in attività di apprendimento che coinvolgono la tecnologia on-line;
- garantire che le comunicazioni digitali dei docenti con alunni e genitori siano svolte nel rispetto del codice di comportamento professionale ed effettuate con sistemi scolastici ufficiali;
- assicurare la riservatezza dei dati personali trattati ai sensi della normativa vigente;
- controllare l'uso delle tecnologie digitali da parte degli alunni durante le lezioni e ogni altra attività scolastica;
- comunicare ai genitori eventuali comportamenti sbagliati dei figli, in relazione all'utilizzo delle risorse digitali, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo.

Alunni

Il ruolo degli alunni include i seguenti compiti:

- essere responsabili, in relazione al proprio grado di maturità e di apprendimento, per l'utilizzo dei sistemi delle tecnologie digitali in conformità con quanto richiesto dai docenti;
- avere una buona comprensione delle potenzialità offerte dalle TIC per la ricerca di contenuti e materiali;
- comprendere l'importanza di adottare buone pratiche di sicurezza on-line quando si utilizzano le tecnologie digitali per non correre rischi;
- adottare condotte rispettose degli altri anche quando si comunica in rete;
- esprimere domande o difficoltà o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o di internet ai docenti e ai genitori.

Genitori

Il ruolo degli alunni include i seguenti compiti:

- Sostenere la scuola nel promuovere la sicurezza online e rispettare le norme stabilite dal documento di E-Policy;
- partecipare agli incontri proposti dalla scuola relativamente alla sicurezza nell'uso di internet e delle tecnologie digitali, con particolare attenzione al fenomeno del cyberbullismo;
- non diffondere dati personali;
- adottare condotte rispettose degli altri quando si comunica in rete;
- rispettare la normativa relativa alla privacy.

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 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.

Condivisione e comunicazione della Policy all'intera comunità scolastica
Oltre alla pubblicazione del documento di E-Policy sul sito della scuola, la Policy sarà comunicata al personale, agli alunni, alla comunità nei seguenti modi.

Condivisione e comunicazione agli alunni:
- tutti gli alunni saranno informati che la rete, l'uso di Internet e di ogni dispositivo digitale saranno controllati dagli insegnanti e utilizzati solo con la loro autorizzazione.
- l'elenco delle regole per la sicurezza on-line sarà pubblicato in tutte le aule o laboratori con accesso a internet;

Condivisione e comunicazione al personale:
- il documento sarà discusso negli organi collegiali;
- il personale riceverà informazione attraverso mail istituzionale ed eventuali corsi di formazione.

Condivisione e comunicazione ai genitori:
- condivisione del documento nelle assemblee di classe;
- incontri formativi.

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.

Gestione delle infrazioni alla Policy
Le potenziali infrazioni in cui è possibile che gli alunni incorrano a scuola nell'utilizzo delle tecnologie digitali di internet di cui si dispone per la didattica, in relazione alla fascia di età considerate, sono prevedibilmente le seguenti:
- il collegamento a siti web non indicati dai docenti;
- utilizzo della rete per interessi privati e personali che esulano dalla didattica;
- scaricare file, video-musicali protetti da copyright;
- deridere, offendere, insultare, calunniare e minacciare attraverso l'uso delle TIC;
- pubblicare sui social network o inviare tramite messaggistica immagini, video o testi che siano offensivi della dignità personale;
- attuare cyberstolking o altre forme di persecuzione e molestia attraverso l'uso delle TIC

Sono previsti pertanto da parte dei docenti provvedimenti "disciplinari" proporzionati all'età e alla gravità del comportamento, quali:
- il richiamo verbale
- il richiamo scritto con annotazione sul diario
- la convocazione dei genitori da parte degli insegnanti
- la convocazione dei genitori da parte del Dirigente scolastico
- La segnalazione alle autorità competenti in caso di reati

Contestualmente sono previsti interventi di carattere educativo di rinforzo dei comportamenti corretti e riparativi dei disagi causati, di prevenzione e gestione positiva dei conflitti.

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.

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 nostro piano d'azioni

Azioni da svolgere:

- Creazione del gruppo di lavoro ePolicy
- Realizzazione di un sistema di monitoraggio delle attività
- Realizzazione di un'assemblea per discutere delle attività di progetto

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.

Curricolo sulle competenze digitali per gli studenti

"La competenza digitale consiste nel saper utilizzare con dimestichezza e spirito critico le tecnologie della società dell'informazione per il lavoro, il tempo libero e la comunicazione. Essa è supportata da abilità di base nelle TIC: l'uso del computer per reperire, valutare, conservare, produrre, presentare e scambiare informazioni nonché per comunicare e partecipare a reti collaborative tramite Internet" (Raccomandazione del Parlamento europeo relativa a competenze chiave per l'apprendimento permanente). Il curricolo della scuola del primo ciclo di istruzione sulle competenze digitali è trasversale alle discipline. Ciascuna classe sviluppa le competenze in un curricolo verticale flessibile, che tiene conto non solo dell'età degli alunni, ma anche dei prerequisiti che gli alunni già possiedono.

NUCLEO TEMATICO	OBIETTIVI	CONOSCENZE E ABILITA'	COMPETENZE	TEMI E CONTENUTI	ATTIVITA'	COLLEGAMENTI INTERDISCIPLINARI
CITTADINANZA DIGITALE Uso consapevole e responsabile dei mezzi di comunicazione virtuali.	-Utilizzare in modo consapevole e responsabile le tecnologie.	-Conoscere ed avvalersi consapevolmente e responsabilmente dei mezzi di comunicazione virtuale -Conoscere i pericoli della rete. -Saper distinguere l'identità digitale da un'identità reale. -Saper applicare le regole sulla privacy, tutelando se stesso e il bene collettivo.	- Fa un uso cosciente delle nuove tecnologie della comunicazione, tenendo conto dei rischi dell'ambiente digitale. -E' consapevole dell'identità digitale, come valore individuale e collettivo da preservare. -Applica le regole sulla privacy.	-I rischi e le insidie dell'ambiente digitale. -Cyberbullismo. -Le regole della privacy. -La *netiquette* (regole di buon comportamento sul web). -Coding (pensiero computazionale)	Le attività, che ogni Consiglio di classe sceglierà di svolgere, potrebbero essere legate ad alcuni dei seguenti appuntamenti curriculari: -Safer internet day -L'ora del Coding	Tecnologia Inglese Italiano Matematica Motoria **CAMPI DI ESPERIENZA PER SCUOLA DELL'INFANZIA:** -I discorsi e le parole -La conoscenza del mondo -Il corpo e il movimento

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.

FORMAZIONE DEI DOCENTI SULL'UTILIZZO E L'INTEGRAZIONE DELLE TIC NELLA DIDATTICA
Il nostro istituto promuove l'utilizzo delle TIC nella didattica, a partire dalle prime aule computer, passando attraverso il piano di implementazione delle LIM. Di pari passo si sono succedute le attività di formazione informatica per tutti i docenti.
Nell'ambito del PNSD questa scuola ha individuato:

- La figura dell'Animatore Digitale con specifiche competenze nell'attuazione degli obiettivi e delle innovazioni previste dal PSND
- Il Team per l'innovazione digitale, composto da dieci docenti, ha la funzione, all'interno dell'istituto, di supportare e accompagnare l'innovazione didattica sia per i docenti che per le famiglie
- La figura di referente per il cyber bullismo con competenze in materia di sicurezza on-line

La scuola ha aderito a:

- Formazione interna riguardante l'uso delle TIC nella didattica

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

La scuola si impegna a promuovere percorsi formativi per gli insegnanti sul tema dell'uso consapevole delle tecnologie digitali e della prevenzione dei rischi online. Ciò avverrà tramite specifici momenti di aggiornamento che, con cadenza, verranno organizzati dall'Istituto scolastico con la collaborazione del personale specializzato interno (animatore digitale, referente bullismo e cyberbullismo) e se necessario del personale esterno (professionisti qualificati), con il supporto della rete scolastica del territorio (USR, Osservatori regionali sul bullismo, scuole Polo, etc...), delle amministrazioni comunali, dei servizi socio-educativi e delle associazioni presenti.
La formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica e la sicurezza in rete costituisce una delle principali priorità della nostra scuola. Il nostro istituto è particolarmente attento ad ogni iniziativa atta a raggiungere un buon livello di formazione in merito all'utilizzo e l'integrazione delle TIC nella didattica a alla sicurezza in rete. Tutti i docenti sono comunque sollecitati e prestare particolare attenzione all'auto formazione continua per rimanere sempre aggiornati in merito ad un mondo in continua evoluzione.
Negli ultimi due anni, nel nostro Istituto sono stati promossi degli incontri con esperti esterni sul tema della sicurezza in rete, rivolti sia agli alunni che alle loro famiglie.

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 darà ampia diffusione, tramite pubblicazione sul sito, del presente documento di policy per consentire alle famiglie una piena conoscenza del regolamento sull'utilizzo delle nuove tecnologie all'interno dell'istituto e favorire un'attiva collaborazione tra la scuola e le famiglie sui temi della prevenzione dei rischi connessi a un uso non consapevole e critico del digitale.
Questo documento rappresenta un altro passo per sensibilizzare le famiglie dei nostri alunni, affinché affrontino in modo consapevole i pericoli della rete stando a fianco ai docenti nelle loro attività didattiche basate sull'uso delle TIC.

L'Istituto sta definendo un protocollo di ulteriori incontri, tenuti da esperti, da attuare annualmente per sensibilizzare le famiglie su cyberbullismo e uso consapevole della rete e delle tecnologie digitali.

Il nostro piano d'azioni

- Organizzare incontri con esperti per i docenti sulle competenze digitali.
- Organizzare incontri con esperti per i genitori sull'educazione alla cittadinanza digitale.
- 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.

Protezione dei dati personali

Il personale scolastico 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).

Tutto il personale incaricato ha ricevuto poi istruzioni particolareggiate, applicabili al trattamento di dati personali su supporto cartaceo, su supporto informatico e attraverso un corso di formazione in presenza ai

fini della protezione e sicurezza degli stessi. I dati personali sono protetti secondo la normativa vigente, viene richiesta specifica autorizzazione per l'utilizzo di foto, video, testi per la documentazione di attività didattiche, anche in occasione di eventi o manifestazioni, e per la pubblicazione sul sito della scuola, Facebook e Canale YouTube.

3.2 - Accesso ad Internet

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

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

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

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

L'accesso ad internet avviene attraverso rete fissa o attraverso wi-fi, al quale si accede con password.
In tutti i computer l'installazione dei programmi è riservata all'amministratore.
Sui computer sono installati programmi antivirus. Anche la navigazione in internet è controllata.
La scuola ha un sito web del quale è responsabile e sul quale vengono pubblicati solo contenuti pertinenti alle finalità educative istituzionali, nel rispetto della tutela della privacy degli studenti e del personale, secondo le disposizioni normative.
La scuola ha una pagina Facebook e un canale YouTube gestiti da docenti FS.
Si usa da anni il Registro Elettronico.

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.

Gestione accessi (password, backup):
Nei computer presenti nelle aule e nei laboratori è prevista una password Utente per accedere al WIFI.

E-mail:
L'account di posta elettronica è solo quello istituzionale utilizzato ordinariamente dagli uffici amministrativi, sia per la posta in ingresso che in uscita. Le credenziali sono in possesso del personale amministrativo.

Sito Web della scuola: https://www.istitutocomprensivovernole.edu.it/.
Tutti i contenuti sono pubblicati direttamente sotto la supervisione del responsabile del sito web FS Area2 che ne valuta con il Dirigente scolastico la sicurezza e l'adeguatezza sotto i diversi profili dell'accessibilità, della pertinenza dei contenuti, del rispetto della privacy.

Social network: Tutti i contenuti utilizzati su Facebook e Youtube vengono preventivamente visionati e selezionati dai docenti in termini di sicurezza e di adattabilità alla programmazione scolastica. L'istituzione scolastica, per nome e per conto della stessa, è autorizzata a utilizzare il canale Youtube e la pagina di Facebook per la diffusione e/o pubblicazione di un evento, previarichiesta di autorizzazione e supervisione del Dirigente Scolastico.

3.4 - Strumentazione personale

I dispositivi tecnologici sono parte integrante della vita personale di ciascuno, compresa quella degli/lle studenti/esse e dei docenti (oltre che di tutte le figure professionali che a vario titolo sono inseriti nel mondo della scuola), ed influenzano necessariamente anche la didattica e gli stili di apprendimento. Comprendere il loro utilizzo e le loro potenzialità innovative, diventa di cruciale importanza, anche considerando il quadro di indirizzo normativo esistente e le azioni programmatiche, fra queste il Progetto Generazioni Connesse e il più ampio PNSD.

La presente ***ePolicy*** contiene indicazioni, revisioni o eventuali integrazioni di Regolamenti già esistenti che disciplinano l'uso dei dispositivi personali in classe, a seconda dei vari usi, anche in considerazione dei dieci punti del Miur per l'uso dei dispositivi mobili a scuola (BYOD, "Bring your own device").

Risulta fondamentale per la comunità scolastica aprire un dialogo su questa tematica e riflettere sulle possibilità per l'Istituto di dotarsi di una regolamentazione condivisa e specifica che tratti tali aspetti, considerando aspetti positivi ed eventuali criticità nella e per la didattica.

Il nostro piano d'azioni

- 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)
- 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 i genitori 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.*

Sensibilizzazione

- Gli operatori della scuola, in modo particolare gli insegnanti, sono promotori e garanti della costruzione dialogica di un percorso formativo partecipato, e nel loro ruolo diventano confidenti degli alunni e delle loro esperienze.
- Gli insegnanti sono spesso i primi a rilevare le problematiche e i rischi che bambini e adolescenti possono trovarsi ad affrontare ogni giorno(casi di bullismo e di cyberbullismo di cui gli insegnanti vengono a conoscenza e che si trovano ad affrontare durante l'anno scolastico).
- E' compito degli insegnanti imparare a riconoscere i rischi più comuni che i ragazzi possono correre sul web, per potere poi intervenire adeguatamente.

Prevenzione

- Internet favorisce la libertà d'espressione e, quando si entra a far parte di una community o di un servizio dove interagiscono più utenti, vanno considerati abusi meritevoli di segnalazione solo i contenuti palesemente impropri o illeciti.
- Quando si inizia a navigare tra i servizi dei Social Network e le applicazioni web tipo YouTube, Facebook, bisogna informarsi subito su quali sono i diritti e i doveri dell'utente, leggendo il regolamento, tenendosi aggiornati, esplorando i siti informativi e istituzionali che affrontano queste tematiche.

- Se si condividono informazioni personali, bisogna farlo scegliendo con cura che cosa rendere pubblico e cosa rendere privato.
- Se si condividono elementi multimediali o informazioni che riguardano più persone è necessario avere il permesso di ciascun utente coinvolto prima di effettuare la pubblicazione.
- Ogni abuso subito o rilevato nella navigazione, deve essere segnalato tramite i canali e gli strumenti offerti dal servizio, indicando in modo semplice i riferimenti per ottenere tempestivamente la rimozione del contenuto. Tutti i social network garantiscono la possibilità di segnalare materiale inopportuno mediante semplici operazioni da compiere direttamente sul sito.

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).

La Legge 71/2017 sulla prevenzione e il contrasto del cyberbullismo attribuisce alle Istituzioni scolastiche nuovi compiti e responsabilità.
La Legge prevede la figura di un coordinatore delle iniziative di prevenzione e contrasto del cyberbullismo, messe in atto dalla scuola.
Tale figura è il referente di Istituto, che ha il compito di coordinare le varie iniziative, avvalendosi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio.

Nel corso di questi anni, nel nostro Istituto sono state portate avanti diverse iniziative, rivolte soprattutto agli alunni delle Scuole Secondarie di Vernole e Castri, grazie alla collaborazione di tuti i docenti e del Dirigente scolastico.
La finalità è stata quella di sensibilizzare i ragazzi riguardo il fenomeno del cyberbullismo, che, negli ultimi anni, purtroppo, si sta diffondendo sempre più, soprattutto nelle scuole.
Le attività si sono svolte sia nelle ore curriculari che extracurriculari e sono state rivolte agli alunni delle classi seconde e terze delle Scuole Secondarie di Vernole e Castri.
La partecipazione è stata cospicua, l'indice di interesse da parte degli allievi e dei genitori è stato alto, perchè si sono visti coinvolti in un tema molto vicino a loro.
I vari aspetti del bullismo e del cyberbullismo sono stati ampiamente illustrati sia dai docenti, nelle singole classi, che da esperti esterni, che sono riusciti a coinvolgere i ragazzi ed i loro genitori, mostrando alcuni aspetti del fenomeno a loro del tutto ignoti.
Inoltre, il nostro Istituto partecipa annualmente al Safer Internet Day, con varie attività e manifestazioni.
Tutte le attività rivolte alla prevenzione del Cyberbullismo continueranno ad essere organizzate nel nostro Istituto.

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.

Con *hate speech* – espressione tradotta normalmente in italiano come "discorsi d'odio" o "espressioni d'odio" o "linguaggio d'odio" – si intende un particolare tipo di comunicazione che si serve di parole, espressioni o elementi non verbali, aventi come fine ultimo quello di esprimere e diffondere odio ed intolleranza, nonché di incitare al pregiudizio e alla paura verso un soggetto o un gruppo di persone accomunate da etnia, orientamento sessuale o religioso, disabilità, appartenenza culturale o sociale, mediante deprecabili modalità di manifestazione del pensiero, diffuse e reiterate attraverso Internet.
Questo fenomeno ha acquisito particolare visibilità ed estensione, con la diffusione dei social network.

Per i rischi connessi all'utilizzo delle nuove tecnologie (grooming, cyberbullismo, furto di identità, sexting, adescamento, hate speech), la scuola:

- organizza una serie di incontri/confronti tra docenti, referente d'Istituto per il Cyberbullismo e gli alunni delle classi quinte della Scuola Primaria e di tutte classi della Scuola Secondaria di I° grado, sul tema della cyber-violenza, dell'uso dei social e della concezione dell'odio da parte dei ragazzi, all'interno della campagna di sensibilizzazione sulla violenza psicologica in ambito giovanile.

- si affida a consulenti esterni per organizzare, come già fatto negli anni precedenti, incontri informativi rivolti agli alunni (Polizia Postale, Carabinieri, Magistrati, Consulenti informatici forensi, Partner di "Generazioni Connesse", Equipe Formazione Territoriale (MIUR), Associazioni del Territorio preposte allo scopo).

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?

I giochi online descrivono qualsiasi videogioco che offra interazioni online con altri giocatori.
Ciò che è ancora diverso da un gioco all'altro è il livello di interazione offerto. Quante informazioni condividono i giocatori e quante persone con cui interagiscono sono i due fattori chiave di cui i genitori devono essere consapevoli.
I giochi online sono importanti da capire perché offrono un'enorme quantità di divertimento lavoro di squadra, collaborazione e avventura immaginativa per i bambini. Giocati in modo sano contribuiscono in modo essenziale allo sviluppo e alla socializzazione dei bambini.
Tuttavia, è importante che i genitori comprendano i giochi online in modo che possano incoraggiare abitudini sicure e sane nei bambini e nella tecnologia fin dalla tenera età.

Il gioco è un modo divertente e socievole di trascorrere del tempo, incoraggiando il lavoro di squadra e lo sviluppo di abilità. Tutte cose buone, ma ci sono alcune cose di cui i genitori devono essere consapevoli:

- Alcuni giochi permettono ai ragazzi di **giocare e chattare con chiunque nel mondo**. Ciò significa che potrebbero imbattersi in un linguaggio offensivo e in fenomeni di bullismo
- **Non tutti online sono quelli che dicono di essere**. I ragazzi dovrebbero evitare di fornire dettagli personali che possano identificarli
- Alcuni **giochi incoraggiano i giocatori ad acquistare elementi extra** durante il gioco - è noto che i bambini accumulano fatture elevate senza accorgersene
- In **casi estremi di bullismo, noto anche come "dolore"**, può essere utilizzato come tattica per vincere partite. I bambini possono trovarsi vittima di bullismo o cyberbullismo
- Non tutti i giochi sono **appropriati per la loro età**
- Può essere **difficile fermare alcuni giochi nel mezzo di una battaglia** poiché ci sono penalità per l'abbandono e i bambini possono sentire che stanno deludendo i compagni di squadra.

Il fenomeno del gioco on line è sempre più diffuso tra i ragazzi, che tendono ad isolarsi e a trascorrere molte ore a giocare, trascurando, in questo modo, le normali attività quotidiane.
Il nostro Istituto, attraverso la progettazione del curricolo di Educazione civica, ha previsto degli interventi a riguardo, che prevedono attività di sensibilizzazione riguardanti questo tema (come diventare giocatori consapevoli on line, il decalogo dell'uso corretto di internet)

4.5 - Sexting

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

La Scuola provvede, anche attraverso incontri con esperti, di informare i genitori circa le possibilità di attivare forme di controllo parentale della navigazione.
Per quanto riguarda gli studenti, prevede l' inserimento nel curricolo di Educazione civica di temi legati all'affettività.
Inoltre, è opportuno ricordare, sia ad alunni che a genitori, che l'invio e la detenzione di foto che ritraggono minorenni in pose sessualmente esplicite configura il reato di distribuzione di materiale pedopornografico.
Manca spesso la consapevolezza, tra ragazzi e adulti, che una foto o un video diffusi in rete divengono di pubblico dominio e la diffusione non è controllabile. In casi di rilevante gravità occorre informare tempestivamente il Dirigente Scolastico.

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.

Sensibilizzazione, attraverso incontri con esperti informatici forensi, sull'esistenza di individui che usano la rete per instaurare relazioni, virtuali o reali, con minorenni e per indurli alla prostituzione. Qualora si venga a conoscenza di casi simili, occorre valutarne la fondatezza e avvisare il Dirigente Scolastico per l'intervento delle forze dell'ordine.

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

- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti.
- Promuovere incontri e laboratori per studenti e studentesse dedicati alla Cittadinanza Digitale e ai temi sulla diversità e l'inclusione.
- Promuovere attività di peer-education sui temi della sicurezza online nella scuola.

Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

Il personale docente del nostro Istituto quando ha il sospetto o la certezza che uno/a studente/essa possa essere vittima o responsabile di una situazione di cyberbullismo, sexting o adescamento online ha a disposizione procedure definite e può fare riferimento a tutta la comunità scolastica.

Questa sezione dell'ePolicy contiene le procedure standardizzate per la segnalazione e gestione dei problemi connessi a comportamenti online a rischio di studenti e studentesse (vedi allegati a seguire).

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

Nelle procedure:

- sono indicate le **figure preposte all'accoglienza della segnalazione e alla presa in carico e gestione del caso**.
- le modalità di coinvolgimento del referente per il contrasto del bullismo e del cyberbullismo, oltre al Dirigente Scolastico.

Inoltre, la scuola **individua le figure che costituiranno un team** preposto alla gestione della segnalazione (gestione interna alla scuola, invio ai soggetti competenti).

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

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

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

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

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

- **Cyberbullismo**: è necessario capire se si tratta effettivamente di cyberbullismo o di altra problematica. Oltre al contesto, vanno considerate le modalità attraverso le quali il comportamento si manifesta (alla presenza di un "pubblico"? Tra coetanei? In modo ripetuto e intenzionale? C'è un danno percepito alla vittima? etc.). È necessario poi valutare l'eventuale stato di disagio vissuto dagli/lle studenti/esse coinvolti/e (e quindi valutare se rivolgersi ad un servizio deputato ad offrire un supporto psicologico e/o di mediazione).
- **Adescamento online**: se si sospetta un caso di adescamento online è opportuno, innanzitutto, fare attenzione a non cancellare eventuali prove da smartphone, tablet e computer utilizzati dalla persona minorenne e inoltre è importante non sostituirsi al bambino/a e/o adolescente, evitando, quindi, di rispondere all'adescatore al suo posto). È fondamentale valutare il benessere psicofisico dei minori e il rischio che corrono. Vi ricordiamo che l'attuale normativa prevede che la persona coinvolta in qualità di vittima o testimone in alcune tipologie di reati, tra cui il grooming, debba essere ascoltata in sede di raccolta di informazioni con l'ausilio di una persona esperta in psicologia o psichiatria infantile.
- **Sexting**: nel caso in cui immagini e/o video, anche prodotte autonomamente da persone minorenni, sfuggano al loro controllo e vengano diffuse senza il loro consenso è opportuno adottare sistemi di segnalazione con l'obiettivo primario di tutelare il minore e ottenere la rimozione del materiale, per quanto possibile, se online e il blocco della sua diffusione via dispositivi mobili.

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

Vi suggeriamo, inoltre, i seguenti servizi:

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

- Clicca e segnala di Telefono Azzurro e STOP-IT di Save the Children Italia per segnalare la presenza di materiale pedopornografico online.

I docenti sono chiamati a predisporre delle rilevazioni e qualora si rendano conto che si trovano di fronte a situazioni di criticità dovranno rivolgersi ai Referenti che avvieranno le procedure con le istituzioni preposte nonché la segnalazione alla Dirigenza Scolastica. Tali rilevazioni avvengono secondo i protocolli suggeriti dalla piattaforma messa a disposizione da "Generazioni Connesse", come da schemi allegati.
Inoltre, ci si potrà avvalere del servizio Hotline che si occupa di raccogliere e dare corso a segnalazioni, inoltrate anche in forma anonima, relative a contenuti pedopornografici e altri contenuti illegali o dannosi, diffusi attraverso la rete.

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.

Il personale della scuola, anche con l'ausilio tecnico dell'Animatore Digitale, provvederà a conservare le eventuali tracce di una navigazione non consentita su internet o del passaggio di materiali inidonei sui pc della scuola, nonché la data e l'ora.
Nel caso di messaggi, si cercherà di risalire al mittente attraverso i dati del suo profilo.
L'insegnante dovrà copiare e stampare i messaggi per fornire le eventuali prove all'indagine sugli abusi commessi e raccogliere testimonianze sui fatti da riferire al Dirigente Scolastico, alla famiglia ed, eventualmente, alla Polizia Postale.
Qualora siano coinvolti più alunni, in qualità di vittime o di responsabili della condotta scorretta, le famiglie degli alunni in questione saranno convocate e informate tempestivamente per un confronto.

In base alla gravità dei fatti si provvederà:
- a una comunicazione scritta tramite diario alle famiglie;
- a una nota disciplinare sul registro on-line;
- a una convocazione formale dei genitori degli alunni, tramite segreteria;
- a una convocazione delle famiglie da parte del Dirigente scolastico;
- per i reati più gravi la scuola si rivolgerà direttamente agli organi di polizia competenti e al Comitato di garanzia.

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.

REGIONE PUGLIA

1. Comitato Regionale Unicef (Sede di Lecce)

Presidente: Maria antonietta Rucco
Segretario: Raffaele Cacchione
Indirizzo: Via Cicolella, 11-Lecce

2. Co.Re.Com. (Comitato Regionale per le Comunicazioni)

In situazione dell'articolo 1, comma 13, della legge 31 Luglio 1997, n. 249, è stato istituito con la Legge Regionale 3/2000 il Comitato regionale per le comunicazioni (Co.Re.Com.) della Regione Puglia, al fine di assicurare a livello territoriale regionale le necessarie funzioni di governo, di garanzia e di controllo in tema di comunicazioni.

Il **CORECOM** è l'organo di governo, garanzia e controllo sul sistema delle comunicazioni in ambito regionale. E' organo funzionale dell'Autorità per le garanzie nelle comunicazioni (AGCOM) e organismo di consulenza della Giunta e del Consiglio regionale della Puglia.
In qualità di organo regionale, svolge funzioni di consulenza, di supporto e di garanzia della Regione per le funzioni ad essa spettanti, secondo le leggi statali e regionali, nel campo della comunicazione
portale ufficiale
http://corecom.consiglio.puglia.it

3.Ufficio Scolastico Regionale

Via Sigismondo Castromediano, 123, 70126 Bari BA

4. Polizia Postale e delle Comunicazioni

La polizia postale e delle comunicazioni è una specialità della Polizia di Stato italiana, preposta al contrasto delle frodi postali e del crimine informatico.
Agenzia principale: Polizia di Stato
Fondazione: 1981
Sede centrale: Roma
Attiva: 1981 – oggi
Tipo: Polizia informatica

5. Aziende Sanitarie Locali

Azienda	Indirizzo	Telefono	Fax	E-mail
114 - ASL BA	LUNGOMARE STARITA 6 - 70123 - BARI - BA	0805842567	0805842563	
106 - ASL BR	VIA NAPOLI 8 - 72100 - BRINDISI - BR	083120561	083120561	protocollo.asl.brindisi@pec.rupar.puglia.it
113 - ASL BT	VIA FORNACI 201 - 70031 - ANDRIA - BT	0883299111	0883299461	
115 - ASL FG	PIAZZA LIBERTÀ 1 - 71100 - FOGGIA - FG	0881731111	0881732619	
116 - ASL LE	VIA MIGLIETTA 5 - 73100 - LECCE - LE	0832215111	0832215648	
112 - ASL TA	VIALE VIRGILIO 31 - 74100 - TARANTO - TA	0997786111	0994585927	direttoregenerale@asl.taranto.it

6. Garante Regionale per l'Infanzia e l'Adolescenza e Difensore Civico:

Ludovico Abbaticchio

Il Garante regionale per i diritti dei minori ha il compito di **promuovere interventi** a favore dei minori, **sensibilizzare sul tema della protezione** dei più piccoli e **assicurare il buon funzionamento dei servizi** rivolti all'infanzia. Nella Regione Puglia, l'Ufficio del Garante per i diritti dei minori è previsto all'art. 30 della legge regionale n. 19 'Disciplina del sistema integrato dei servizi sociali per la dignità e il benessere delle donne e degli uomini di Puglia' ed è istituito presso il Consiglio regionale. All'Ufficio del Garante è affidata la **protezione e la tutela non giurisdizionale** dei diritti dell'infanzia, degli adolescenti e dei minori residenti o temporaneamente presenti sul territorio regionale.

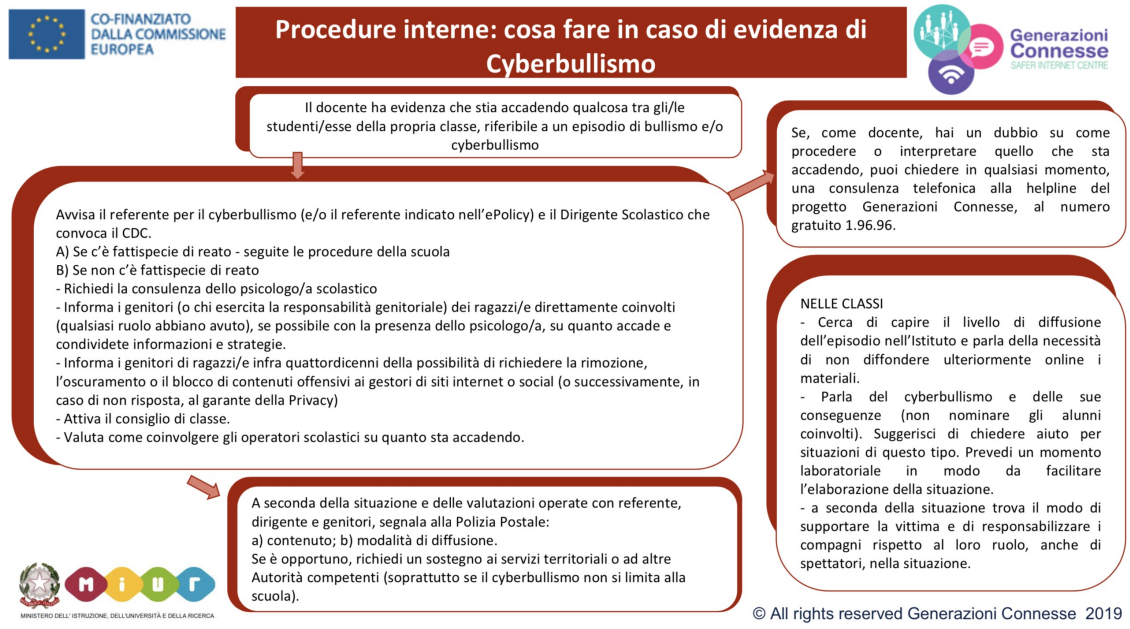
7. Tribunale per i Minorenni

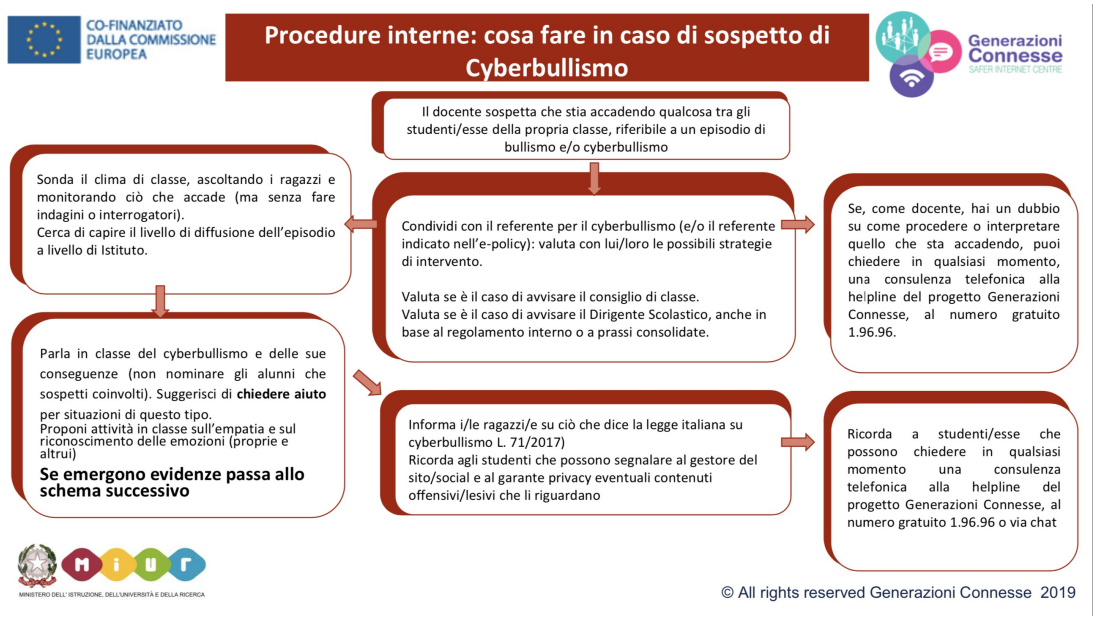
PUGLIA		
BARI	**Tribunale per i Minorenni di BARI**	Province di: Bari, Barletta-Andria-Trani, Foggia.
	Via Tommaso Fiore, 49 – 70123 BARI (BA)	
	www.giustizia.it - TM di Bari	
	www.tribunaleperiminorennidibari.it	

	E-mail: **tribmin.bari@giustizia.it**	
	Tel. 080.5744133 – 080.57441357	
	fax: 080.5794607 – 080.5743169	
LECCE	**Tribunale per i Minorenni di LECCE**	Province di: Lecce, Brindisi.
	Via Dalmazio Birago s.n.c. 73100 – LECCE (LE)	
	www.giustizia.it - TM di Lecce	
	E-mail: **tribmin.lecce@giustizia.it**	
	Tel. 0832.2131	
	fax: 0832.307874	
TARANTO	**Tribunale per i Minorenni di TARANTO**	Provincia di Taranto.
	Piazza Duomo – Palazzo santachiara – 74100 TARANTO (TA)	
	www.giustizia.it - TM di Taranto	
	E-mail: **tribmin.taranto@giustizia.it**	
	Tel. 099.7343111 (centralino) – 099.7343558	
	fax: 099.7343551 / 553	

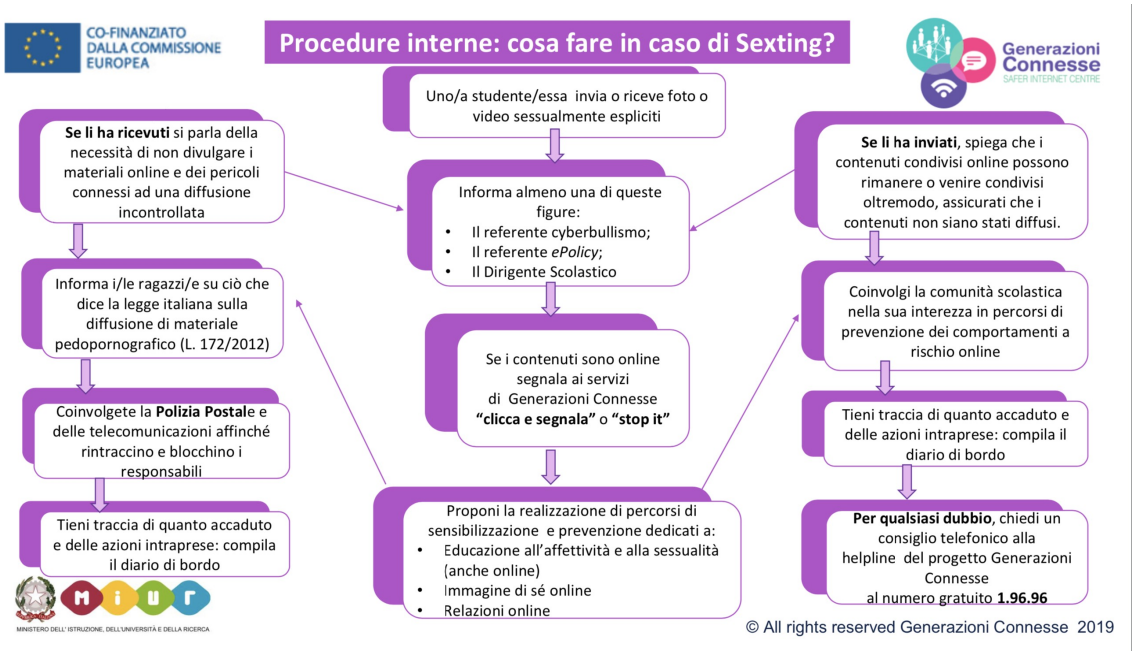
5.4. - Allegati con le procedure

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

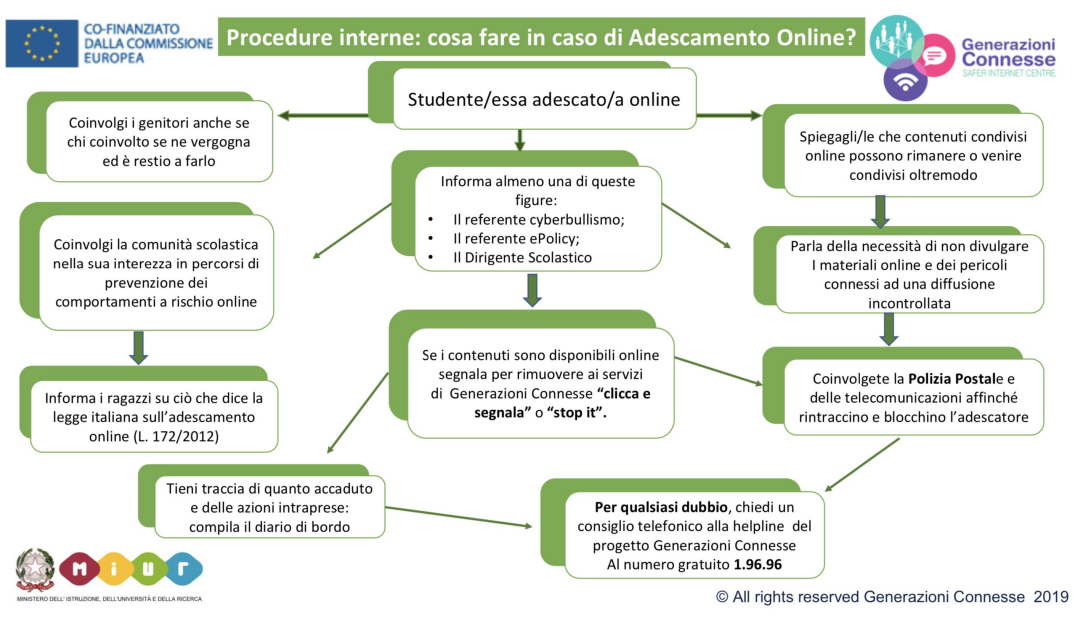




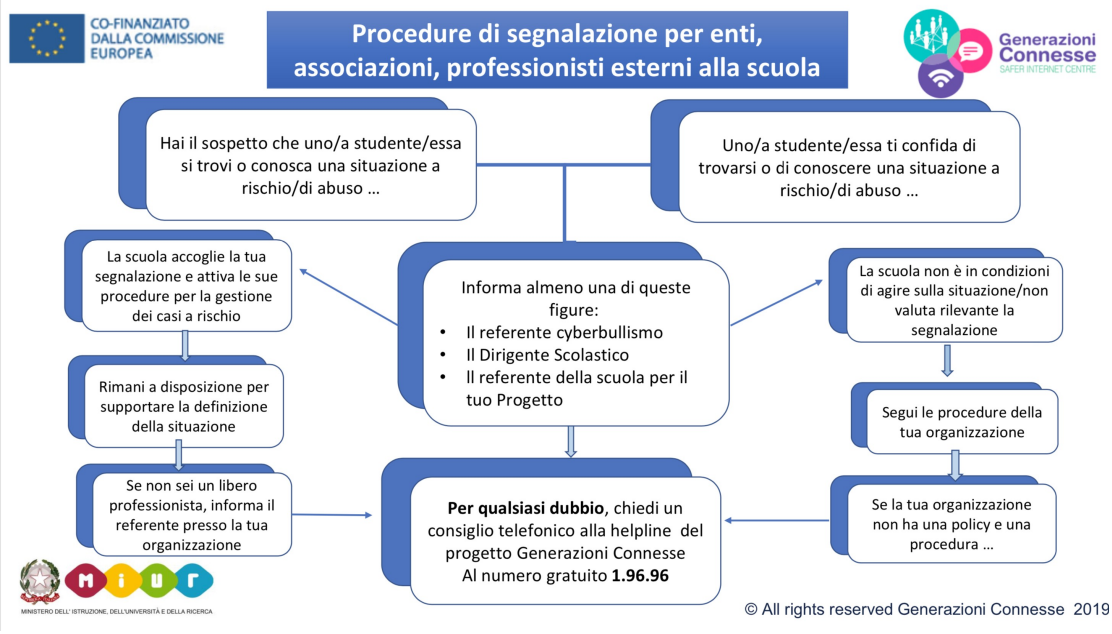
Procedure interne: cosa fare in caso di sexting?



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

- organizzazione di Corsi di formazione per docenti, genitori, operatori del settore socioeducativo;
- partecipazione da parte di docenti, studenti e genitori a convegni e seminari sul tema del bullismo e del cyberbullismo;
- interventi di consulenza e supporto, relativamente a casi di cyberbullismo (su richiesta da parte della scuola).