DOCUMENTO DI E-POLICY

(Approvato in CD del 13.12.21 e CI del 15.12.21)

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 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.

1.2 Argomenti del Documento

A) Presentazione dell'ePolicy
Scopo dell'ePolicy
Ruoli e responsabilità
Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica
Gestione delle infrazioni alla ePolicy
Monitoraggio dell'implementazione dell'ePolicy e suo aggiornamento
Integrazione dell'ePolicy con regolamenti esistenti

B) Formazione e curricolo
Curricolo sulle competenze digitali per gli studenti
Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica
Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali
Sensibilizzazione delle famiglie e Patto di corresponsabilità

C) Gestione dell'infrastruttura e della strumentazione ICT (Information and Communication Technology) della e nella scuola
Protezione dei dati personali
Accesso ad Internet
Strumenti di comunicazione online
Strumentazione personale

D) Rischi on line: conoscere, prevenire e rilevare
Sensibilizzazione e prevenzione
Cyberbullismo: che cos'è e come prevenirlo
Hate speech: che cos'è e come prevenirlo
Dipendenza da Internet e gioco online
Sexting
Adescamento online
Pedopornografia

E) Segnalazione e gestione dei casi
Cosa segnalare
Come segnalare: quali strumenti e a chi
Gli attori sul territorio per intervenire

1.3 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-Safety 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 Digitale emanate dal Miur; salvaguardare e proteggere i ragazzi e il personale dell'Istituto con la promozione dell'uso consapevole e critico, da parte degli studenti 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; assistere il personale della scuola affinché lavori in modo sicuro e responsabile; impostare chiare aspettative di comportamento e/o codici di condotta rilevanti per un uso responsabile di Internet a scopo didattico, personale o ricreativo; affrontare gli abusi online come il cyberbullismo; garantire che tutti i membri della comunità scolastica siano consapevoli del fatto che il comportamento illecito o pericoloso è inaccettabile e che saranno intraprese le opportune azioni disciplinari e giudiziarie. Gli utenti, soprattutto minori, devono essere pienamente consapevoli dei rischi a cui si espongono quando navigano in rete. E' altissima la probabilità 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.

1.4 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:

- rispettare il presente regolamento e la normativa vigente;
- tutelare la propria privacy, quella degli altri adulti e quella degli studenti;
- rispettare la "netiquette", galateo della rete.

Dirigente Scolastico

Il ruolo del Dirigente scolastico nel promuovere l'uso consentito delle tecnologie e di internet include i seguenti compiti: la responsabilità generale per i dati e la sicurezza dei dati; garantire che la scuola utilizzi un Internet Service filtrato approvato, 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 e per la formazione di altri colleghi; essere a conoscenza delle procedure da seguire in caso di infrazione della E–Safety Policy; ruolo di primo piano nello stabilire e rivedere la E-Safety Policy; ricevere relazioni di monitoraggio periodiche della sicurezza online da parte del responsabile; garantire che vi sia un sistema in grado di monitorare il personale di supporto che svolge le procedure di sicurezza online interne.

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 uso improprio o a dannosi attacchi esterni;
- garantire il funzionamento dei diversi canali di comunicazione della scuola (sportello, circolari, sito web, ecc.) all'interno della scuola e fra la scuola e le famiglie degli alunni per la notifica di documenti e informazioni del Dirigente scolastico e dell'Animatore Digitale nell'ambito dell'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, nonché proporre la revisione delle politiche dell'istituzione con l'individuazione di soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola;
- assicurare che gli utenti possano accedere alla rete della scuola solo tramite password personali applicate e regolarmente cambiate e curare la manutenzione e lo sviluppo del sito web della scuola per scopi istituzionali e consentiti (istruzione e formazione);
- coinvolgere la comunità scolastica (alunni, genitori e altri attori del territorio) nella partecipazione ad attività e progetti attinenti la "scuola digitale".

Team digitale

Il ruolo del Team digitale include i seguenti compiti:

- pubblicare e diffondere la E-Safety 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 (alunni, genitori e altri attori del territorio) nella partecipazione ad attività e progetti attinenti la "scuola digitale".

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'utilizzo delle tecnologie digitali, dispositivi mobili, macchine fotografiche, ecc. da parte degli alunni durante le lezioni e ogni altra attività scolastica (ove consentito);
- nelle lezioni in cui è programmato l'utilizzo di Internet, guidare gli alunni a siti controllati e verificati come adatti per il loro uso e controllare che nelle ricerche su Internet siano trovati e trattati solo materiali idonei;
- comunicare ai genitori difficoltà, bisogni o disagi espressi dagli studenti (ovvero valutazioni sulla condotta non adeguata degli stessi) rilevati a scuola e connessi all'utilizzo delle TIC, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo;
- segnalare qualsiasi problema o proposta di carattere tecnico-organizzativo ovvero esigenza di carattere informativo all'Animatore Digitale ai fini della ricerca di soluzioni metodologiche e tecnologiche innovative da diffondere nella scuola e di un aggiornamento della politica adottata in materia di prevenzione e gestione dei rischi nell'uso delle TIC;
- segnalare al Dirigente Scolastico e ai genitori qualsiasi abuso rilevato a scuola nei confronti degli studenti in relazione all'utilizzo delle tecnologie digitali o di internet, per l'adozione delle procedure previste dalle norme.

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 a quanto richiesto dai docenti; avere una buona comprensione delle

potenzialità offerte dalle TIC per la ricerca di contenuti e materiali ma anche della necessità di evitare il plagio e rispettare i diritti d'autore; comprendere l'importanza di adottare buone pratiche di sicurezza on-line quando si utilizzano le tecnologie digitali per non correre rischi;
- adottare condotte rispettose degli altri anche quando si comunica in rete;
- esprimere domande, difficoltà o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o di internet ai docenti e ai genitori.

Genitori
- sostenere la scuola nel promuovere la sicurezza online e approvare l'accordo di E- Safety Policy con la scuola;
- partecipare agli incontri proposti dalla scuola relativamente alla sicurezza nell'uso di internet e delle tecnologie digitali e al cyberbullismo;
- non diffondere dati personali;
- adottare condotte rispettose degli altri quando si comunica in rete;
- conoscere le norme di utilizzo della rete nel rispetto del copyright e del diritto di autore
- rispettare la normativa relativa alla privacy.

1.6 Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto
Tutti gli altri operatori presenti a qualsiasi titolo nella scuola (esperti esterni, collaboratori, ditte esterne ...) dovranno attenersi alle norme previste per il personale scolastico. Si allegano schede operative fornite dalla piattaforma "Generazioni connesse" per la rilevazione e la gestione dei casi. I documenti relativi alle procedure operative e i protocolli da siglare con le istituzioni del territorio sono in via di definizione ed approvazione

1.7 Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica
Il documento di E-policy viene condiviso con tutta la comunità educante, ponendo al centro gli studenti e le studentesse e sottolineando compiti, funzioni e attività reciproche. È molto importante che ciascun attore scolastico (dai docenti agli/lle studenti/esse) si faccia a sua volta promotore del documento.
L'E-policy viene condivisa e comunicata al personale, agli studenti e alle studentesse, alla comunità scolastica attraverso:
- la pubblicazione del documento sul sito istituzionale della scuola;
- il Patto di Corresponsabilità, che deve essere sottoscritto dalle famiglie e rilasciato alle stesse all'inizio dell'anno scolastico;

Il documento è approvato dal Collegio dei Docenti e dal Consiglio di Istituto e viene esposto in versione semplificata negli spazi che dispongono di pc collegati alla Rete o comunque esposto in vari punti spaziali dell'Istituto.
Gli studenti e le studentesse vengono informati sul fatto che sono monitorati e supportati nella navigazione on line, negli spazi della scuola e sulle regole di condotta da tenere in Rete.

1.8 Condivisione e comunicazione della Policy all'intera comunità scolastica
Oltre alla pubblicazione della E-Safety Policy sul sito della scuola, la Policy sarà comunicata al personale, agli alunni, alla comunità nei seguenti modi:
a) 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.
b) l'istruzione degli alunni riguardo all'uso responsabile e sicuro di internet precederà l'accesso alla rete.
c) l'elenco delle regole per la sicurezza on-line sarà pubblicato in tutte le aule o laboratori con accesso a internet;
d) 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".
e) il documento sarà discusso negli organi collegiali;
f) il personale riceverà informazione attraverso materiali pubblicati sul sito della scuola e corsi di formazione;
g) condivisione del documento nelle assemblee di classe;
h) incontri formativi.

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

Le 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
- utilizzare la rete per interessi privati e personali che esulano dalla didattica (scaricare file, video-musicali protetti da copyright)
- deridere, offendere, insultare, calunniare attraverso l'uso delle TIC; 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 R.E.
- la convocazione dei genitori da parte degli insegnanti
- la convocazione dei genitori da parte del Dirigente scolastico
- la sospensione dalle lezioni
- la segnalazione agli assistenti sociali
- 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, di promozione di rapporti amicali e di reti di solidarietà, di promozione della conoscenza e della gestione delle emozioni.
L'infrazione della presente e-policy da parte del personale (docente, ATA,) può costituire elemento di contestazione d'addebito disciplinare e per gli esterni (esperti, collaboratori, etc.) può essere causa di risoluzione di eventuali contratti e/o convenzioni in essere.

1.10 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

L'E-policy viene aggiornata periodicamente e quando si verificano cambiamenti significativi in riferimento all'uso delle tecnologie digitali all'interno della scuola. Le modifiche del documento saranno discusse con tutti i membri del personale docente. Il monitoraggio del documento sarà realizzato a partire da una valutazione della sua efficacia in riferimento agli obiettivi specifici che lo stesso si pone.
Il monitoraggio dell'implementazione della Policy e del suo eventuale aggiornamento sarà svolto ogni anno. Il monitoraggio sarà affidato al referente del bullismo/cyberbullismo e al suo gruppo di lavoro.
L'aggiornamento della policy sarà curato dal Dirigente Scolastico, dal referente del bullismo/cyber bullismo e dal suo gruppo di lavoro, sulla base delle segnalazioni effettuate dal personale della scuola

1.11 Integrazione dell'ePolicy con Regolamenti esistenti

Il Regolamento dell'Istituto Scolastico viene aggiornato con specifici riferimenti all'E-policy, così come anche il Patto di Corresponsabilità, in coerenza con le Linee Guida Miur e le indicazioni normative generali sui temi in oggetto. Il presente documento si integra con gli obiettivi e i contenuti dei seguenti documenti: PTOF e Regolamento d'Istituto. Il referente del bullismo/cyberbullismo con il suo gruppo di lavoro, in collaborazione con la Commissione PTOF, in raccordo con il Collegio Docenti, opera al fine di integrare i regolamenti dell'Istituto con il presente documento, per le eventuali e opportune modifiche da proporre al Consiglio d'Istituto.

Piano di azioni - Azioni da svolgere entro un'annualità scolastica:

- Creazione del gruppo di lavoro ePolicy (Azione sviluppabile nel breve periodo)
- Realizzazione di un sistema di monitoraggio delle attività (Azione sviluppabile nell'arco di un anno)
- Organizzazione di un'assemblea per discutere delle attività di progetto (Azione sviluppabile nell'arco di un anno).

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 sviluppare 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.
Considerato che la competenza digitale è una delle competenze chiave per l’apprendimento permanente, identificata dall’Unione Europea, l’uso delle TIC per l’apprendimento è ormai indispensabile. “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 nell’uso delle tecnologie informatiche: l’utilizzo 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 secondo 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, ma anche dei prerequisiti che gli studenti già possiedono.

Area sillabo ECD	**Anno**	**Contenuti**	**Tempi**	**Discipline coinvolte**
Educazione all’informazione	Biennio	Come funzionano i motori di ricerca e vari siti didattici generalisti gestiti da studenti	Anno scolastico	Tutte le discipline
Educazione ai media	Biennio	Conoscenza dei rischi della Rete. Elementi normativi sulla tutela della privacy. Normativa di base sull’utilizzo dei social network Approfondimento dei concetti di netiquette, flame, tag…	Anno scolastico	Tutte le discipline
Educazione all’informazione	Biennio	Come valutate l’attendibilità nell’aggiornamento di un sito	Anno scolastico	Tecnico-scientifiche
Educazione all’informazione	Biennio	Costruire cartelle e sottocartelle organizzare e classificare contenuti digitali	Anno scolastico	Tutte le discipline
Educazione all’informazione	Triennio	Come si rielaborano le informazioni (no plagio) Come citare le fonti; come mettere link e creareuna sitografia; file condivisi	Anno scolastico	Tutte le discipline
Cultura e creatività Digitale	Triennio	Creazione di PPT, Fogli di calcolo, conoscenza e uso di siti web, app	Anno scolastico	Tecnico-scientifiche
Cultura e creatività Digitale	Triennio	Coding robotica	Anno scolastico	Tecnico-scientifiche

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.
Il nostro istituto promuove l’utilizzo delle tecnologie 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, alla formazione generalizzata per tutti i docenti per l’uso delle LIM, capillarmente diffuso nei nostri

plessi, all'attuale percorso formativo relativo al Coding, che ha visto partecipazione massiccia. Il corpo docente è sensibile al tema del cyberbullismo e parteciperà a momenti formativi sul tema. Nell'ambito del PNSD questa scuola ha individuato:
L'Animatore Digitale con specifiche competenze nell'attuazione degli obiettivi e delle innovazioni previste dal PSND;

- il Team per l'innovazione digitale, composto da tre docenti, due assistenti amministrativi e una unità del personale ATA, ha la funzione di supportare e accompagnare l'innovazione didattica nelle istituzioni scolastiche e l'attività dell'Animatore Digitale.
- un docente con funzioni di web-master al quale fare riferimento per qualsiasi problema connesso con l'uso delle TIC;
- il referente per il cyber bullismo con competenze in materia di sicurezza on-line.

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.

2.3 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 gli studenti 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 il primo passo per sensibilizzare le famiglie degli studenti affinché affrontino in modo consapevole i pericoli della rete nell'uso delle tecnologie informatiche
L'Istituto definirà un protocollo di incontri, tenuti da esperti o da docenti formati, da attuare annualmente per sensibilizzare le famiglie su cyberbullismo e uso consapevole della rete e delle tecnologie digitali.

Piano di azioni (da sviluppare nell'arco dell'anno scolastico 2021/2022

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

Piano di azioni (da sviluppare nell'arco dei tre anni scolastici successivi)

- Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare incontri con esperti per i docenti sulle competenze digitali.
- Organizzare incontri con esperti per i genitori sull'educazione alla cittadinanza digitale.

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 tal senso, 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, conformi alla normativa vigente, in materia di 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 riceve poi istruzioni particolareggiate applicabili al trattamento di dati personali su supporto cartaceo e su supporto informatico, 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

L'accesso a Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale.

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.

Il diritto fondamentale di accesso a Internet deve essere assicurato nei suoi presupposti sostanziali e non solo come possibilità di collegamento alla Rete.

L'accesso comprende la libertà di scelta per quanto riguarda dispositivi, sistemi operativi e applicazioni anche distribuite.

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.

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, in questo caso si accede attraverso una procedura di autorizzazione che richiede una password. Nei computer portatili si accede attraverso una password e 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.

Sito web della scuola: La scuola ha un sito web del quale è responsabile. La scuola pubblicherà sul proprio sito web i contenuti che saranno valutati come pertinenti alle finalità educative istituzionali, ponendo attenzione alla tutela della privacy degli studenti e del personale, secondo le disposizioni normative vigenti.
È in uso usa da alcuni anni il Registro Elettronico.

3.3 Strumenti di comunicazione on line

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, ecc.): Nei computer presenti nelle aule e nei laboratori sarà 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.giorgifermi.edu.it/. Tutti i contenuti del settore didattico sono pubblicati direttamente sotto la supervisione del responsabile del sito web 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, ecc...

3.4 Strumentazioni personali

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.
Per gli studenti: Come da Regolamento d'Istituto agli studenti è vietato l'utilizzo del cellulare all'interno della scuola. Non è richiesto l'uso di altra strumentazione personale.
Per i docenti e per il personale della scuola: I docenti e il personale della scuola possono utilizzare i propri cellulari in orario di lavoro solo per emergenze. I docenti possono usare i propri devices per scopi didattici a integrazione dei dispositivi scolastici a disposizione.

Il nostro piano d'azioni (da sviluppare nell'arco dell'anno scolastico 2021/2022).

- 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)

Il nostro piano d'azioni (da sviluppare nell'arco dei tre anni scolastici successivi).

- Organizzare incontri per la consultazione degli studenti/studentesse su indicazioni/regolamenti sull'uso dei dispositivi digitali personali
- Organizzare incontri per la consultazione dei genitori su indicazioni/regolamenti sull'uso dei dispositivi digitali personali
- 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
- 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)

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 sè 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 conseguenze 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 degli studenti.

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 studenti e delle loro esperienze. Proprio per questo, gli insegnanti sono spesso i primi a rilevare le problematiche e i rischi che studenti e gli adolescenti possono trovarsi ad affrontare ogni giorno. Si pensi ai numerosi 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

Principi generali della 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 e non tutti quei contenuti con cui semplicemente non si è d'accordo o non piacciono.
- Quando si inizia a navigare tra i servizi dei Social Network e le applicazioni web tipo YouTube, Facebook, etc., 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. E' indispensabile scegliere con attenzione le amicizie con cui accrescere la propria rete e i gruppi a cui aderire, proteggendo la propria identità digitale con password complesse e usando una domanda di recupero password dalla risposta non banale.
- 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. Non bisogna pubblicare su YouTube video dove sono presenti persone filmate senza il loro consenso.
- Bisogna contribuire a rendere il Web un luogo sicuro, pertanto ogni volta che un utente commette involontariamente un abuso o un errore, pubblicando del materiale illecito, non idoneo o offensivo, bisogna contattarlo e fornire le spiegazioni relative alle regole, diffondendo così i principi della sicurezza.
- 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 (abuso, data, ora, utenti e servizio coinvolti). Tutti i social network garantiscono la possibilità di segnalare materiale inopportuno mediante semplici operazioni da compiere direttamente sul sito. Prima di trasformare un incidente o una "bravata" in una denuncia alle autorità competenti avvalersi della modalità di segnalazione che non obbliga le parti in causa a conseguenze penali e giudiziarie che possono durare anni.

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 istituzione 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 progettare azioni preventive ed educative e non solo sanzionatorie.

Il Referente per le iniziative di prevenzione e contrasto 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).

Si definisce cyberbullismo qualunque forma di aggressione, molestia, ricatto, pressione, ingiuria, denigrazione, diffamazione, furto d'identità, trattamento illecito di dati personali realizzata per via telematica a danno di minorenni. A questo si aggiunge inoltre la diffusione su web di contenuti aventi come oggetto uno o più componenti della famiglia del minore.

Le novità introdotte dalla recente legge e i compiti affidati dalla stessa alle scuole comportano delle modifiche al Regolamento di Istituto e al Patto di Educativo di Corresponsabilità. I regolamenti scolastici dovranno prevedere misure di prevenzione ed esplicite sanzioni disciplinari, commisurate alla gravità degli atti compiuti. Il dirigente attiva, nei confronti dello/gli studente/i che ha/hanno commesso atti di cyberbullismo, azioni non di carattere punitivo ma educativo.

Il Dirigente Scolastico che venga a conoscenza di atti di cyberbullismo informa tempestivamente i genitori dei minori coinvolti. Episodi di cyberbullismo e presenza di materiale pedopornografico online possono essere segnalati al servizio Helpline di Telefono Azzurro 1.96.96, una piattaforma integrata finalizzata ad aiutare i ragazzi e le ragazze a comunicare il proprio disagio e alla Hotline "Stop-It" di Save the Children, all'indirizzo www.stop-it.it. Le segnalazioni vengono successivamente trasmesse al Centro Nazionale per il Contrasto alla Pedopornografia su Internet, istituito presso la Polizia Postale e delle Comunicazioni, per consentire le attività di investigazione necessarie. (LINEE DI ORIENTAMENTO per la prevenzione e il contrasto del cyberbullismo, ottobre 2017).

Azioni

I docenti si impegnano a:

- accompagnare gli alunni nella navigazione in Rete, coinvolgendoli nell'esplorazione delle opportunità e dei rischi, con attività calendarizzate dall'inizio dell'anno;
- approfondire, con attività mirate in classe, la conoscenza del fenomeno del bullismo e del cyber bullismo;
- creare degli spazi in cui gli alunni si possano confrontare su questo tema, utilizzando come spunti di riflessione: spezzoni di film, canzoni, materiali prodotti da altri studenti;
- confrontarsi con gli altri insegnanti della classe, della scuola o con esperti del territorio; rivolgersi alla helpline di generazioni connesse (www.generazioniconnesse.it).

I genitori si impegnano a:

- firmare il patto di Corresponsabilità redatto dalla scuola; prendere visione della E-Safety Policy;
- seguire le azioni promosse dalla scuola per un uso corretto della rete;
- frequentare corsi di formazione/convegni che la scuola organizzerà per la diffusione di informazioni legate ad un uso corretto della tecnologia digitale.

Gli alunni si impegnano a:

- prendere visione della E-Safety Policy pubblicata sul sito web della scuola; rispettare le regole per un uso corretto della tecnologia;
- denunciare qualsiasi caso di abuso online;
- prendere parte a qualsiasi evento che la scuola organizza in materia di sicurezza online.

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 è 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.

L'hate speech – espressione tradotta normalmente in italiano come "discorsi d'odio" o "espressioni d'odio" o "linguaggio d'odio" – consiste in una specifica forma di discriminazione che si estrinseca non attraverso azioni o omissioni, ma mediante deprecabili modalità di manifestazione del pensiero. Diffuse e reiterate attraverso Internet, tali forme espressive hanno l'effetto di alimentare i pregiudizi, consolidare gli stereotipi e rafforzare l'ostilità di taluni gruppi di persone, solitamente in maggioranza o in posizione di dominanza in un determinato contesto sociale, nei confronti di altri gruppi con diverse caratteristiche, in genere minoritari.

Per i rischi connessi all'utilizzo delle nuove tecnologie (grooming, cyberbullismo, furto di identità, sexting, adescamento, hate speech), la scuola si affida a consulenti esterni per organizzare incontri informativi rivolti agli alunni (Polizia Postale, Carabinieri, 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?

La dipendenza da internet e dal gioco online può rappresentare una vera e propria patologia che compromette la salute e le relazioni sociali e che in taluni casi (per es. uso della carta di credito a insaputa di altri) rappresenta un vero e proprio illecito.

Divieto per gli alunni di utilizzare propri dispositivi digitali in classe ad eccezione di specifiche e regolamentate attività didattiche.

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. Si prevede, verso i genitori l'informazione circa le possibilità di attivare forme di controllo parentale della navigazione; verso gli studenti: inserimento nel curricolo di temi legati all'affettività, alla sessualità e alle differenze di genere. In casi simili, se l'entità è lieve occorre in primo luogo parlarne con alunne e alunni e rispettivi genitori, ricordando loro 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 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.

In casi simili, se l'entità è lieve occorre in primo luogo parlarne con studentesse, studenti e rispettivi genitori, ricordando loro che l'invio e la detenzione di foto che ritraggono minorenni in pose sessualmente esplicite configura il reato di distribuzione di materiale pedopornografico. Chi è immerso dalla nascita nelle nuove tecnologie spesso non è consapevole che una foto o un video diffusi in rete potrebbero non essere tolti mai più né è consapevole di scambiare o diffondere materiale pedopornografico. In casi di rilevante gravità occorre informare tempestivamente il Dirigente Scolastico per gli adempimenti del caso.

AZIONI

- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti agli/lle studenti/studentesse, con il coinvolgimento di esperti.
- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti.
- Promuovere incontri e laboratori per studenti e studentesse dedicati all' Educazione Civica Digitale.
- Organizzare uno o più incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/lle studenti/studentesse.
- Organizzare uno o più eventi e/o dibattiti in momenti extra-scolastici, sui temi della diversità e sull'inclusione rivolti a genitori, studenti/studentesse e personale della scuola.
- Pianificare e realizzare progetti di peer-education - sui temi della sicurezza online - nella scuola.

5. SEGNALAZIONE E GESTIONE DEI CASI

5.1 Cosa segnalare

Il personale docente del nostro Istituto quando ha il sospetto o la certezza che un/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.

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 dai/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 all'adolescente, evitando, quindi, di rispondere all'adescatore al suo posto). È fondamentale valutare il benessere psicofisico dei minori e il rischio che corrono. 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/dannosi diffusi attraverso la rete. I due servizi messi a disposizione dal Safer Internet Center sono il "Clicca e di Telefono Azzurro e "STOP IT" di Save the Children. Una volta ricevuta la segnalazione, gli operatori procederanno a coinvolgere le autorità competenti in materia.
La pubblicazione dei seguenti dati e contenuti

- dati sensibili o riservati (foto, immagini, video personali, informazioni private proprie o di amici; l'indirizzo di casa o il telefono, ecc.);
- contenuti che possano considerarsi in qualche modo lesivi dell'immagine altrui (commenti offensivi, minacce, osservazioni diffamatorie o discriminatorie, foto o video denigratori, videogiochi che contengano un'istigazione alla violenza, ecc.);
- contenuti riconducibili alla sfera sessuale: messaggi, immagini o video a sfondo sessuale, come foto di nudo o semi-nudo, ecc.

andrà opportunamente segnalati per gli interventi opportuni.

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.
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:

- 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, potrà individuare 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 R.E. alle famiglie

- a una nota disciplinare sul registro on-line;
- a una convocazione formale dei genitori degli alunni, tramite segreteria;
- 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.

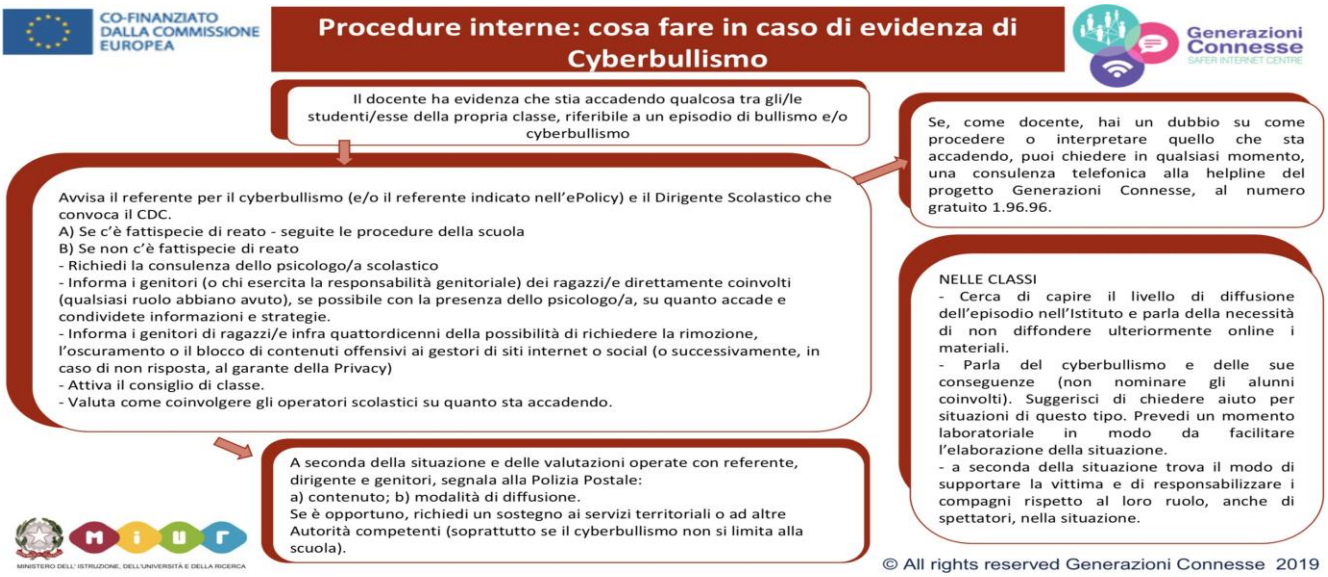
Aziende Sanitarie Locali: forniscono supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in Rete.

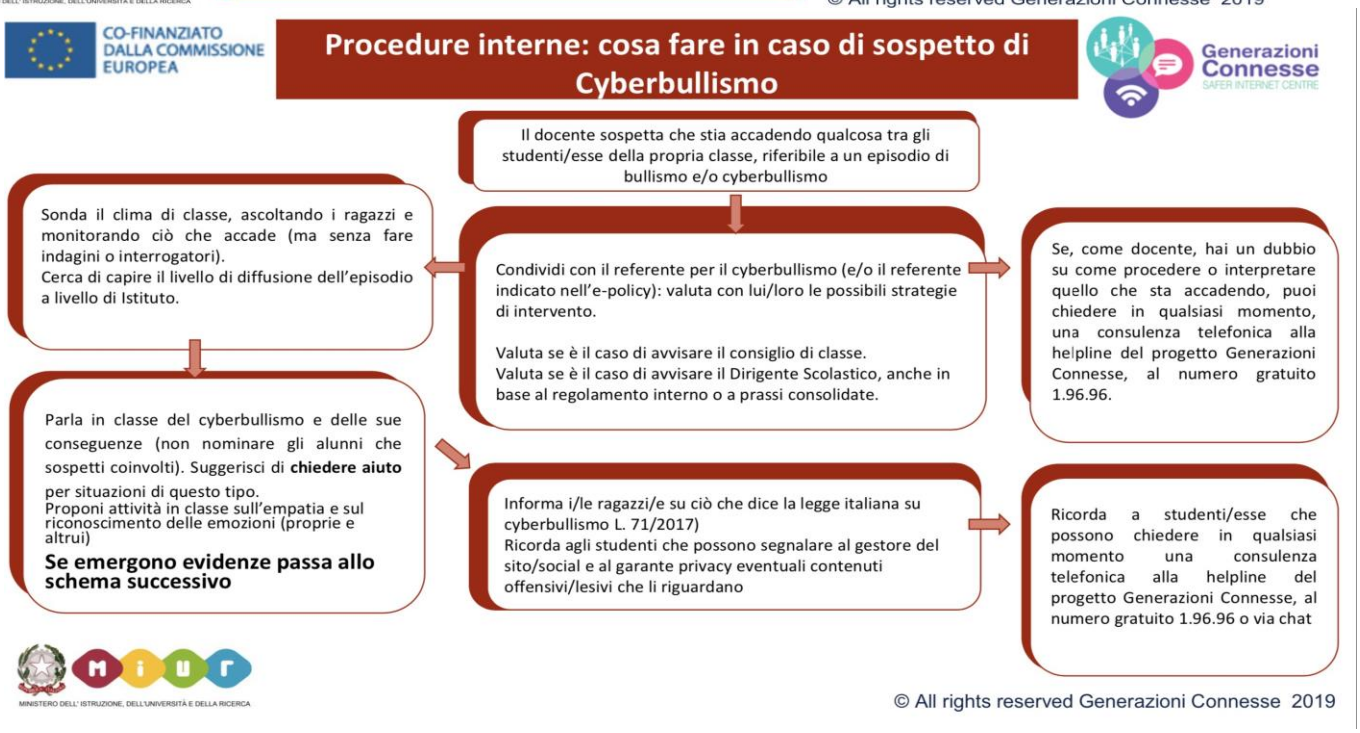
Garante Regionale per l'Infanzia e l'Adolescenza e Difensore Civico: segnalano all'Autorità Giudiziaria e ai Servizi Sociali competenti; accolgono le segnalazioni di presunti abusi e forniscono informazioni sulle modalità di tutela e di esercizio dei diritti dei minori vittime. Segnalano alle amministrazioni 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.

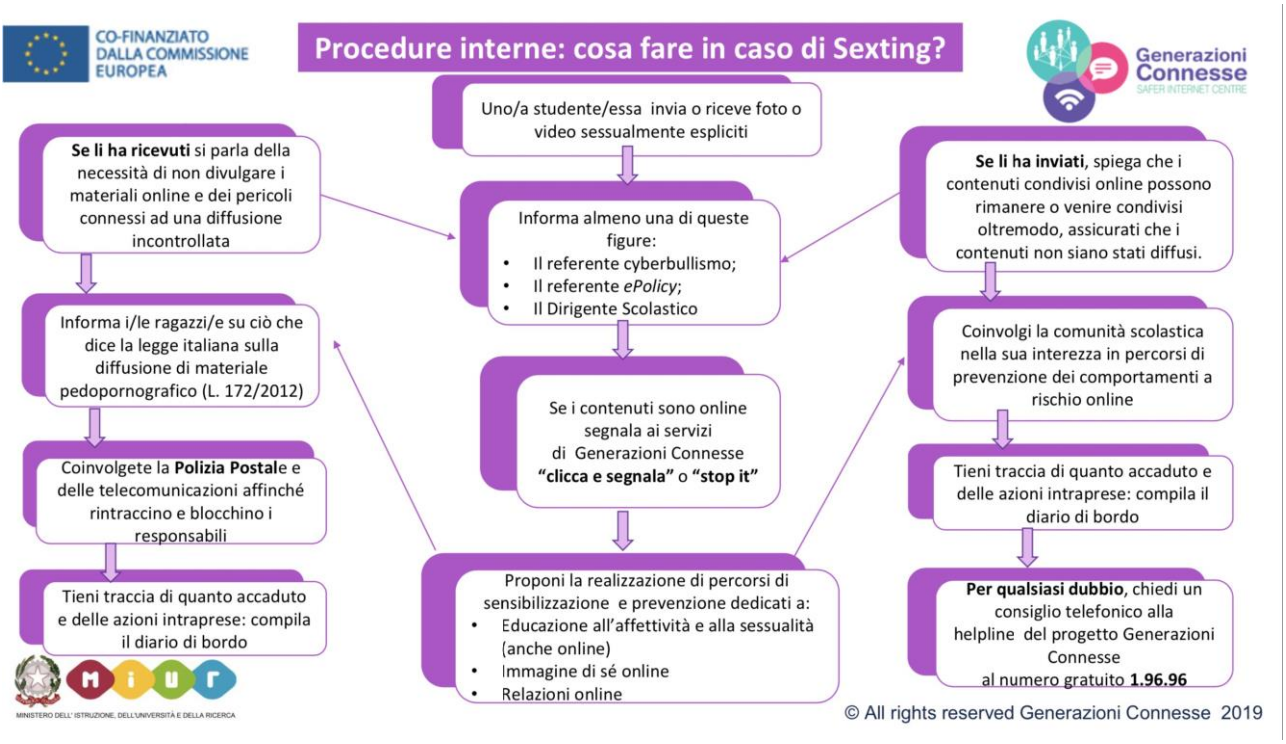
ALLEGATI CON LE PROCEDURE

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

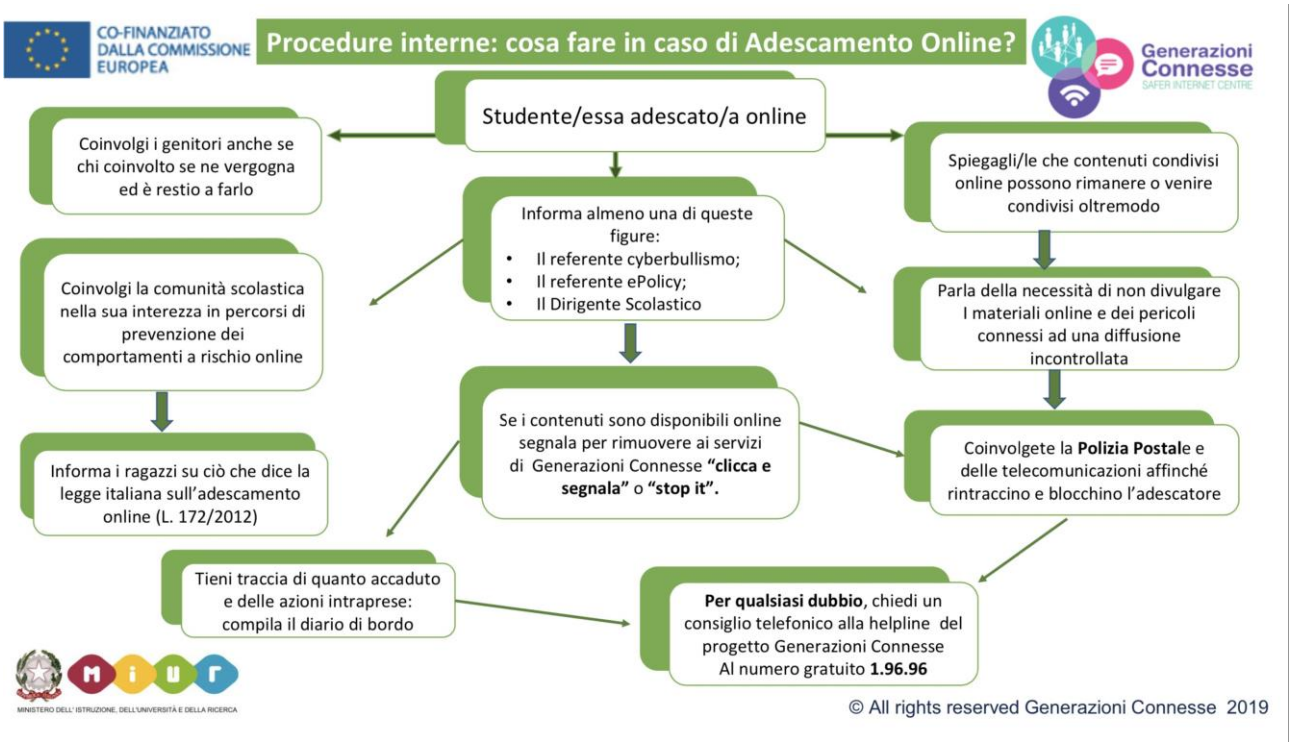




Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



Procedure di segnalazione per enti, associazioni, professionisti esternialla scuola