Documento di ePolicy

NARH09000Q

IPSSEOA "RAFFAELE VIVIANI"C/MMARE

VIA ANNUNZIATELLA 23 - 80053 - CASTELLAMMARE DI STABIA - NAPOLI (NA)

Giuseppina Principe

Capitolo 1 - Introduzione al documento di ePolicy

1.1 - Scopo dell'ePolicy

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

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

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

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

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

Argomenti del Documento

Perché è importante dotarsi di una E-policy?

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

all'uso di Internet.

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

Il nostro Istituto riconosce il valore e le opportunità offerte dalle TIC nel sostenere l'insegnamento, promuovere la creatività, stimolare la consapevolezza e migliorare l'apprendimento degli studenti, ma è ben consapevole dei rischi relativi e della conseguente necessità di fronteggiarli adeguatamente. Con tale premessa, al presente documento E-policy vengono assegnate le seguenti finalità:

- esprimere l'intento educativo e l'offerto formativa dell'Istituto in merito alle TIC e promuoverne un uso corretto e positivo;
- sviluppare l'uso responsabile della rete e delle applicazioni a scopo didattico;
- regolamentare i comportamenti e definire procedure chiare e condivise per la prevenzione, la rilevazione e il contrasto alle problematiche legate ad un uso non consapevole delle tecnologie digitali o ad abusi *online* come il cyberbullismo;
- diffondere tra tutti i membri della comunità scolastica la consapevolezza che a fronte di comportamenti illeciti o pericolosi saranno intraprese appropriate azioni sanzionatorie;
- tutelare tutte le figure scolastiche nell'utilizzo delle tecnologie digitali.

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.

Dirigente Scolastico:

- garantisce la sicurezza online della comunità scolastica;
- promuove la cultura della sicurezza online;
- contribuisce all'organizzazione dei percorsi formativi specifici per tutte le figure scolastiche sull'utilizzo positivo e responsabile delle TIC;
- assicura che il sito web della scuola includa informazioni sulla cultura della sicurezza *online*, rilevanti e condivise con i diversi *stakeholder*;
- organizza il monitoraggio ed il controllo interno della sicurezza *online;*
- controlla e vigilare su fenomeni di hacking ai danni delle reti e dei computer dell'Istituto e la corretta gestione dei dati amministrativi;

in sinergia con il ***DSGA***:

- gestisce dati e informazioni
- assicura nei limiti delle risorse finanziarie disponibili l'intervento di tecnici per garantire che l'infrastruttura tecnologica della scuola sia funzionante, sicura, non aperta ad un uso improprio o a dannosi attacchi esterni;
- favorisce il funzionamento dei diversi canali di comunicazione all'interno della scuola e fra la scuola e le famiglie;
- garantisce che i dati di gestione siano correttamente e opportunamente inseriti e tempestivamente aggiornati.

Animatore e Team dell'Innovazione Digitale:

- promuovono la formazione interna negli ambiti di sviluppo della scuola digitale e forniscono consulenza e informazioni al personale in relazione ai rischi online e alle misure di prevenzione e gestione degli stessi;
- monitorano e rilevano le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di Internet a scuola;
- assicurano che gli utenti possano accedere alla rete della scuola solo tramite password applicate e regolarmente cambiate;
- curano la manutenzione e lo sviluppo del sito web della scuola per scopi istituzionali e consentiti;
- coinvolgono la comunità scolastica nella partecipazione ad attività e progetti attinenti alla scuola digitale;
- promuovono l'inserimento dell'educazione all'uso consapevole delle TIC e alla sicurezza online nel curricolo di Istituto;
- collaborano con personale tecnico interno e consulenti esterni.

Referente Cyberbullismo e ***team di lavoro***:

- prendono parte ai corsi di formazione al fine di garantire l'acquisizione di idonee competenze teoriche e pratiche;
- pubblicizzano attività formative per i docenti;
- favoriscono la conoscenza del fenomeno e gli strumenti di prevenzione dello stesso affinché le famiglie possano riconoscerlo ed intervenire in modo corretto;
- sostengono le famiglie e i minori vittime del cyberbullismo;

in sinergia con il ***DS***:

- definiscono gli interventi di prevenzione del bullismo (per questa funzione partecipano anche il presidente del Consiglio di istituto e i rappresentanti degli studenti);
- intervengono nelle situazioni acute di bullismo.

Docenti:

- leggono, accettano e condividono la e-Policy dell'Istituto;

- diffondono la cultura dell'uso responsabile delle TIC e della Rete;
- educano alla sicurezza online nello svolgimento della propria disciplina;
- vigilano sull'accesso alla Rete da parte degli studenti durante le attività didattiche;
- monitorano e supportano gli alunni quando sono impegnati in attività di apprendimento che prevedono l'uso di dispositivi tecnologici connessi alla Rete;
- segnalano problematiche e comportamenti non adeguati legati all'uso di dispositivi tecnologici connessi alla Rete nonché episodi di bullismo e/o cyberbullismo.

Personale Amministrativo, Tecnico e Ausiliario:

- legge, accetta e condivide la e-Policy dell'Istituto;
- garantisce supporto tecnico a studenti e docenti per usufruire adeguatamente di laboratori, dispositivi digitali e Rete;
- partecipa alle attività di formazione e autoformazione in tema di corretto utilizzo della Rete;
- segnala comportamenti non adeguati legati all'uso di dispositivi tecnologici alla Rete e/o episodi di bullismo e cyberbullismo.

Alunni:

- leggono, accettano e condividono la e-Policy dell'Istituto;
- acquisiscono consapevolezza delle opportunità e dei potenziali rischi della Rete e della comunicazione tramite l'uso di dispositivi tecnologici ad essa connessi;
- applicano le regole basilari della comunicazione e del comportamento in Rete;
- adottano buone pratiche di sicurezza per tutelare la propria privacy e quella dei propri compagni e per proteggersi da possibili dai rischi on line;
- segnalano l'abuso, l'uso improprio o l'accesso a materiali inappropriati;
- partecipano in modo propositivo a progetti ed attività che riguardano l'uso positivo delle TIC e della Rete e farsi promotori di quanto appreso anche in una dimensione di peer education;
- segnalano comportamenti non adeguati legati all'uso di dispositivi tecnologici connessi alla Rete nonché e/o episodi di bullismo e cyberbullismo.

Genitori:

- leggono, accettano e condividono la e-Policy dell'Istituto;
- partecipano in modo propositivo alle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete;
- vigilano sull'utilizzo di dispositivi tecnologici connessi alla Rete adottando i suggerimenti e le condizioni d'uso delle TIC indicate dai docenti;
- comunicano problematiche e preoccupazioni legate all'uso inadeguato e/o non consapevole delle TIC, della Rete e dei dispositivi digitali personali;
- utilizzano in modo consapevole e responsabile i dispositivi digitali e la Rete

ogni qual volta si relazionano con l'Istituto;
- consentono l'utilizzo da parte della scuola di immagini fotografiche e video a fini di promulgazione/documentazione didattica e partecipazione a progetti/concorsi promossi da Enti di affermata reputazione in ambito educativo o territoriale.

Enti educativi esterni e Associazioni

- leggono, accettano e condividono la e-Policy dell'Istituto;
- si uniformano alla politica dell'Istituto riguardo all'uso consapevole della Rete e delle TIC;
- promuovono comportamenti sicuri, la sicurezza online e assicurano la tutela degli studenti e delle studentesse durante le attività di cui sono responsabili;
- utilizzano in modo consapevole e responsabile i dispositivi digitali e la Rete ogni qual volta si relazionano con l'Istituto.

1.3 - Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto

Tutti gli attori che entrano in relazione educativa con gli studenti e le studentesse devono: mantenere sempre un elevato profilo personale e professionale, eliminando atteggiamenti inappropriati, essere guidati dal principio di interesse superiore del minore, ascoltare e prendere in seria considerazione le opinioni ed i desideri dei minori, soprattutto se preoccupati o allertati per qualcosa.

Sono vietati i comportamenti irrispettosi, offensivi o lesivi della privacy, dell'intimità e degli spazi personali degli studenti e delle studentesse oltre che quelli legati a tollerare o partecipare a comportamenti di minori che sono illegali, o abusivi o che mettano a rischio la loro sicurezza.

Tutti gli attori esterni sono tenuti a conoscere e rispettare le regole del nostro Istituto dove sono esplicitate le modalità di utilizzo dei propri dispositivi personali (smartphone, tablet, pc, etc.) e quelli in dotazione della scuola, evitando un uso improprio o comunque deontologicamente scorretto durante le attività con gli studenti e le studentesse. Esiste l'obbligo di rispettare la privacy, soprattutto dei soggetti minorenni, in termini di fotografie, immagini, video o scambio di contatti personali (numero, mail, chat, profili di social network).

Pertanto i soggetti esterni che erogano attività formative ed educative nell'Istituto sono tenuti a:

- leggere, accettare e sottoscrivere la e-Policy dell'Istituto;

- promuovere e garantire la sicurezza on line durante le attività di cui sono responsabili;
- vigilare sull'accesso alla Rete da parte degli studenti durante le attività di cui sono responsabili;
- monitorare e supportare gli alunni quando sono impegnati in attività che prevedono l'uso di dispositivi tecnologici connessi alla Rete;
- utilizzare in modo consapevole e responsabile i dispositivi digitali e la Rete ogni qual volta si relazionano con l'Istituto;
- applicare in modo rigoroso la normativa sulla privacy ed il Regolamento d'Istituto, ponendo particolare attenzione, soprattutto in presenza di soggetti minorenni, al rispetto della privacy in termini di fotografie, immagini, video o scambio di contatti personali (numero, mail, chat, profili di social network);
- segnalare ai docenti referenti e al Dirigente scolastico eventuali comportamenti non adeguati legati all'uso di dispositivi tecnologici connessi alla Rete nonché e/o episodi di bullismo e cyberbullismo.

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

Il documento di E-policy viene condiviso con tutta la comunità educante, ponendo al centro gli studenti e le studentesse e sottolineando compiti, funzioni e attività reciproche. È molto importante che ciascun attore scolastico (dai docenti agli/lle studenti/esse) si faccia a sua volta promotore del documento.

L'E-policy viene condivisa e comunicata al personale, agli studenti e alle studentesse, alla comunità scolastica attraverso:

- la pubblicazione del documento sul sito istituzionale della scuola;
- il Patto di Corresponsabilità, che deve essere sottoscritto dalle famiglie e rilasciato alle stesse all'inizio dell'anno scolastico;

Il documento è approvato dal Collegio dei Docenti e dal Consiglio di Istituto e viene esposto in versione semplificata negli spazi che dispongono di pc collegati alla Rete o comunque esposto in vari punti spaziali dell'Istituto.

Gli studenti e le studentesse vengono informati sul fatto che sono monitorati e supportati nella navigazione on line, negli spazi della scuola e sulle regole di condotta da tenere in Rete.

Il documento è esposto anche nelle bacheche delle sedi coordinate.

Il personale di nuova nomina ed i nuovi alunni riceveranno la e-Policy insieme agli altri documenti da sottoscrivere all'atto della stipula del contratto o dell'iscrizione.
Per tutto il personale sono previsti aggiornamenti ed attività di formazione in materia di sicurezza online.

1.5 - Gestione delle infrazioni alla ePolicy

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

Qualsiasi sospetto, rischio, uso improprio o violazione sarà riferita direttamente al Dirigente Scolastico e, nel caso di situazioni acute di bullismo al Dirigente scolastico e/o al Referente cyberbullismo e ai docenti che compongono il Team Antibullismo.
Il Dirigente avrà cura di convocare le parti interessate e, nei casi necessari, riferirà direttamente alle autorità di competenza.
In ogni caso verrà coinvolta la componente genitori.
Le sanzioni, riferite soprattutto agli alunni, avranno come carattere preferenziale quello educativo/riabilitativo al fine di rafforzare il senso di responsabilità e ripristinare rapporti corretti nell'ambito della comunità scolastica.
Le potenziali infrazioni in cui potrebbero incorrere gli alunni nell'utilizzo delle TIC e della Rete, la natura delle sanzioni e la loro procedura di irrogazione sono contenute nel Regolamento d'Istituto.

La gestione delle infrazioni alla e-Policy da parte del personale scolastico e le relative procedure sanzionatorie sono quelle previste dalla disciplina contrattuale.

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.

Inoltre viene aggiornato anche il Protocollo d'Istituto per la prevenzione e il contrasto dei fenomeni di bullismo e cyberbullismo.

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 Dirigente scolastico con il Team dell'Innovazione Digitale, il gruppo di lavoro ed il Referente cyberbullismo viene incaricato di valutare, periodicamente, l'opportunità di revisionare e/o aggiornare il documento di e-Policy.

Il nostro piano d'azioni

Azioni (da sviluppare nell'arco dell'anno scolastico 2023/2024):

- Organizzare un evento di presentazione del progetto Generazioni Connesse rivolto agli studenti
- Organizzare un evento di presentazione del progetto Generazioni Connesse rivolto ai docenti
- Organizzare un evento di presentazione del progetto Generazioni Connesse rivolto ai genitori

Azioni (da sviluppare nei 3 anni scolastici successivi):

- Organizzare un evento di presentazione e conoscenza dell'ePolicy rivolto agli studenti
- Organizzare un evento di presentazione e conoscenza dell'ePolicy rivolto ai docenti
- Organizzare un evento di presentazione e conoscenza dell'ePolicy rivolto ai genitori

Capitolo 2 - Formazione e curricolo

2.1. Curricolo sulle competenze digitali per gli studenti

I ragazzi usano la Rete quotidianamente, talvolta in modo più "intuitivo" ed "agile" rispetto agli adulti, ma non per questo sono dotati di maggiori "competenze digitali".

Infatti, "la competenza digitale presuppone l'interesse per le tecnologie digitali e il loro utilizzo con dimestichezza e spirito critico e responsabile per apprendere, lavorare e partecipare alla società. Essa comprende l'alfabetizzazione informatica e digitale, la comunicazione e la collaborazione, l'alfabetizzazione mediatica, la creazione di contenuti digitali (inclusa la programmazione), la sicurezza (compreso l'essere a proprio agio nel mondo digitale e possedere competenze relative alla cybersicurezza), le questioni legate alla proprietà intellettuale, la risoluzione di problemi e il pensiero critico" ("Raccomandazione del Consiglio europeo relativa alla competenze chiave per l'apprendimento permanente", C189/9, p.9).

Per questo la scuola si impegna a portare avanti percorsi volti a promuovere tali competenze, al fine di educare gli studenti e le studentesse verso un uso consapevole e responsabile delle tecnologie digitali. Ciò avverrà attraverso la progettazione e implementazione di un curricolo digitale.

L'IPSSEOA Raffaele Viviani ha già inserito attività di educazione digitale all'interno del curricolo di Educazione civica e nelle UdA progettate per il perseguimento delle competenze di area generale e dell'area di indirizzo del PECUP mentre, sulle tematiche del bullismo e del cyberbullismo, sono stati svolti dei moduli PON e sono stati organizzati incontri e seminari con Istituzioni del territorio.

È proprio a partire da tali iniziative che si progetterà un curricolo digitale continuativo e trasversale alle varie discipline nel quale coinvolgere tutte le classi dell'Istituto e che, tenendo conto delle azioni previste dal PNSD, si articoli nelle aree di competenza individuate dal Quadro delle Competenze Europee digitali per i Cittadini.

Il Curricolo che si intende progettare svilupperà le diverse aree di competenza presentando contenuti e attività via via più complessi per consentire alle studentesse e

agli studenti di acquisire livelli di padronanza sempre più elevati.

Il tema che si ritiene più urgente affrontare è quello della **sicurezza** vista non solo come competenza digitale ma anche, e forse soprattutto, come competenza chiave. In tema di sicurezza è infatti possibile individuare competenze digitali connesse alla competenza alfabetica funzionale e multilinguistica, alla competenza matematica, alle competenze sociali e civiche ed alla competenza in materia di consapevolezza ed espressione culturali.

Le metodologie previste dal Curricolo digitale non potranno che essere di tipo laboratoriale in modo che le studentesse e gli studenti siano spinti, in tutte le attività proposte, ad agire e sviluppare le proprie competenze in un ambiente che integri le esperienze quotidiane con l'uso corretto e consapevole delle TIC, della Rete e dei dispositivi digitali.

Il percorso educativo sarà sviluppato in termini di contenuti, abilità e competenze in maniera trasversale dai docenti di ciascun consiglio di classe ma non sono esclusi contributi forniti da professionisti esterni.

Il Curricolo espliciterà per le varie Aree di competenza descrittori e livelli di padronanza in modo da rendere trasparente ed univoca la valutazione.

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.

Tutti i docenti dell'IPSSEOA Raffele Viviani, in conformità con quanto previsto dal piano triennale dell'offerta formativa, hanno svolto attività di formazione inerente all'uso delle nuove tecnologie a supporto della didattica, incrementando le competenze digitali di base in loro possesso.

Nello specifico, visto che l'Istituto utilizza già da diversi anni il registro elettronico e la piattaforma Google Workspace per condividere materiali e risorse tra docenti e con gli alunni, sono stati seguiti corsi di formazione ad hoc ai quali si sono affiancati diverse iniziative di formazione gestite dai docenti del Team per l'innovazione digitale.

Una costante attività di peer education è svolta dal Team per l'innovazione digitale e dai docenti specializzati nell'uso delle tecnologie informatiche in servizio nell'Istituto.

Infine, un certo numero di docenti si è avvalsa dei corsi di aggiornamento riguardanti l'innovazione didattica e la didattica digitale promossi dall'Ambito Territoriale 21 e di quelli presenti sulla piattaforma SOFIA.

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

La scuola si impegna a promuovere percorsi formativi per gli insegnanti sul tema dell'uso consapevole delle tecnologie digitali e della prevenzione dei rischi online. Ciò avverrà tramite specifici momenti di aggiornamento che, con cadenza, verranno organizzati dall'Istituto scolastico con la collaborazione del personale specializzato interno (animatore digitale, referente bullismo e cyberbullismo) e se necessario del personale esterno (professionisti qualificati), con il supporto della rete scolastica del territorio (USR, Osservatori regionali sul bullismo, scuole Polo, etc…), delle amministrazioni comunali, dei servizi socio-educativi e delle associazioni presenti.

L'Istituto inserirà nel Piano triennale dell'offerta formativa specifici momenti di formazione permanente:

- percorsi di autoaggiornamento personali o collettivi;
- iniziative seminariali con professionisti-esperti interni ed esterni alla scuola;
- giornate di approfondimento in accordo con la rete scolastica del territorio (USR, Osservatori regionali sul bullismo, scuole Polo, etc…), le amministrazioni comunali, i servizi socio-educativi e le associazioni/enti presenti;
- momenti formativi di approfondimento con la famiglia e gli/le studenti/studentesse in modo da sensibilizzare l'intera comunità educante sul corretto uso delle tecnologie digitali e sulle potenzialità della Rete.

Infine, in un'area specifica del sito dell'Istituto, saranno messi a disposizione materiali per l'aggiornamento sull'utilizzo consapevole e sicuro di Internet ed il link del progetto "**Generazioni connesse**" nel quale reperire ulteriori approfondimenti, spunti per approfondimenti ed utili strumenti.

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.

Il Patto di corresponsabilità è un documento fondamentale per una comunità educante in quanto nasce da una reciproca assunzione di responsabilità e impegna entrambe le componenti a condividerne i contenuti e a rispettarne gli impegni.

L'Istituto si impegna ad integrare tale documento, insieme al regolamento scolastico, con specifici riferimenti all'uso delle tecnologie digitali e all'ePolicy al fine di informare, rendere partecipi le famiglie sul percorso che si vuole intraprendere con il documento e il piano d'azione e, in ultimo, rafforzare l'alleanza educativa tra scuola e famiglia.

Saranno inoltre previsti incontri fra genitori e specialisti (docenti, forze dell'ordine) per la diffusione del materiale informativo su queste tematiche e favoriti momenti di confronto e discussione anche sulle dinamiche che potrebbero instaurarsi fra i pari con l'uso di cellulari e smartphone o delle chat line o social network più diffusi, con particolare riferimento alla prevenzione del cyberbullismo.

Infine, in un'area specifica del sito dell'Istituto, saranno disponibili tutte le informazioni e le procedure contenute nel documento di e-Policy relative al regolamento sull'utilizzo delle nuove tecnologie all'interno dell'istituto e alla prevenzione dei rischi legati a un

utilizzo non corretto di internet nonché il link del progetto **“Generazioni connesse”** nel quale reperire ulteriori approfondimenti, spunti per approfondimenti ed utili strumenti didattici.

Il nostro piano d'azioni

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

- Effettuare un’analisi del fabbisogno formativo del corpo docente sull’utilizzo e l’integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi sull’utilizzo e l’integrazione delle TIC nella didattica.

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

- 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.

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

3.1 - Protezione dei dati personali

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

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

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

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

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

In questo paragrafo dell'ePolicy affrontiamo tale problematica, con particolare

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

Il nostro Istituto si è prontamente adeguato alla normativa in materia di protezione dei dati personali adempiendo a quanto in essa prescritto. La normativa di riferimento in materia di trattamento dei dati personali è il D. lgs. 196/2003, modificato dal D.lgs. 101/2018, e il GDPR Regolamento EU 679/2016.

Di seguito sono riportate alcune linee guida di e-safety:

- in fase di iscrizione degli alunni alla scuola e agli anni scolastici successivi, i genitori sottoscrivono un'informativa sul trattamento dei dati personali in ottemperanza all'art. 13 D.Lgs 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali);

- l'accesso ai dati riportati nel registro elettronico (ritardi, assenze, note e valutazioni) è riservato ai genitori dell'Istituto, tramite l'invio di una password di accesso strettamente personale.

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.

Il nostro Istituto è dotato di una rete wireless destinata all'utilizzo didattico da parte del corpo docente.
La scuola abilita l'accesso alla rete dei dispositivi personali e consegna di una password allo scopo di estendere il servizio e permettere al personale in oggetto di accedere a contenuti e materiali in rete per consentire l'applicazione di una didattica innovativa e più coinvolgente per gli studenti.

Per gli alunni l'accesso alla rete internet, utilizzando la rete cablata, è permesso nei laboratori e negli spazi adibiti in quanto utilizzano device connessi alla rete wireless. Ciascun utente connesso alla rete dovrà rispettare il presente regolamento e la legislazione vigente, tutelare la propria e altrui privacy, nel rispetto della Netiquette.

La componente studentesca e tutto il personale, dovrà impegnarsi a rispettare le norme di buon utilizzo che la scuola si impegna a redigere e a divulgare prima che sia concesso l'accesso a Internet.

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.

Per facilitare la comunicazione interna ed esterna, lo scambio di informazioni utili e aggiornamenti relativi all'attività scolastica, il nostro Istituto si avvale dei seguenti strumenti di comunicazione online:

Sito web della scuola

Il sito web della scuola (www.alberghieroviviani.edu.it) costituisce la principale interfaccia dell'Istituto. Esso prevede un'area pubblica in cui sono reperibili le informazioni che non comportano la diffusione di dati personali o riservati relative ad avvisi e scadenze, iniziative, organigramma della scuola, albo online e amministrazione trasparente, modulistica.

Registro elettronico

Il registro elettronico *Argo DidUp* consente di gestire tutto quanto concerne la didattica (registro di classe, attività e argomenti della lezione, compiti, annotazioni, note disciplinari, assenze, ritardi, uscite anticipate, condivisione documenti), le comunicazioni di Istituto, collegiali, di classe, individuali (*Bacheca*) e la comunicazione con le famiglie le quali, attraverso le proprie credenziali di accesso, possono visualizzare informazioni utili in merito all'andamento scolastico dei propri figli (ritardi, assenze, note e valutazioni).

Piattaforma Google Workspace for Education

La piattaforma "Google Workspace for Education" fornisce una serie di applicazioni dedicate alla comunicazione e al lavoro condiviso e collaborativo che consentono di gestire in modo efficace il flusso didattico all'interno dell'Istituto.

I principali applicativi utilizzati sono:

Gmail, alla componente alunni che al personale docente e ATA è stata fornita una casella di posta elettronica interna al dominio @alberghieroviviani.edu.it.
Tutti, personale scolastico e studenti, sono invitati a utilizzare solo account di posta elettronica presenti nel dominio scolastico e per scopi inerenti lo svolgimento didattico al fine di consentire l'attivazione di protocolli di controllo.

Classroom, per la creazione e gestione di classi virtuali.

Drive, per l'archiviazione e condivisione di documentazione didattica.

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.

Essendo convinzione generale e condivisa che l'utilizzo delle TIC in ambito didattico debba essere valorizzato, incentivato e orientato costruttivamente, è consentito l'utilizzo di dispositivi personali (smartphone, tablet e PC), come previsto dal Regolamento d'Istituto, previa autorizzazione e sotto la supervisione dell'insegnante presente in aula, solo per attività di insegnamento, funzionali all'insegnamento e di formazione. Ogni altro utilizzo, diverso da quante espressamente indicato nel Regolamento, costituisce infrazione.

Durante l'orario di servizio al personale scolastico è consentito l'utilizzo del cellulare solo per scambio di comunicazioni attinenti alle attività educativo-didattiche e di organizzazione scolastica.

La strumentazione fornita dalla scuola, notebook e PC nelle aule, nei laboratori o nelle postazioni informatiche, va utilizzata con il massimo rispetto e cura. Qualora dovessero verificarsi malfunzionamenti o guasti dei dispositivi tecnologici, bisogna darne tempestiva segnalazione al responsabile del laboratorio o di plesso.

Qualora si utilizzino a scuola dispositivi di archiviazione esterna di proprietà personale (chiavette usb, dischi fissi portatili) è bene controllare preventivamente che essi siano esenti da virus per evitare di danneggiare le attrezzature comuni.

Il nostro piano d'azioni

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

- 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).
- 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).

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

La nostra scuola ha già organizzato eventi riguardanti la sicurezza informatica per gli alunni. Nei prossimi anni scolastici intende:

- Organizzare uno o più eventi o attività volti a formare gli studenti, le studentesse, i Docenti e il personale ATA 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 gli studenti e le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity).

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

4.1 - Sensibilizzazione e Prevenzione

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

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

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

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

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

Il nostro Istituto intende perseguire azioni di sensibilizzazione, prevenzione e contrasto ai rischi e pericoli online legati anche al fenomeno del cyberbullismo, principalmente nelle classi prime e seconde dell'Istituto, in sinergia con la rete dei servizi territoriali locali (Polizia postale, Polizia di Stato).
Tali attività sono necessarie per fornire agli studenti e alle studentesse gli strumenti

necessari per un uso consapevole e responsabile delle tecnologie e dei social media.

Quest'anno è stata prevista la realizzazione di uno sportello virtuale, raggiungibile mediante un codice QRcode, utile alla segnalazione di episodi di bullismo, cyberbullismo e problematiche legate ai rischi della rete, nel rispetto dell'anonimato. E' stato inoltre realizzato un progetto PON proprio sul tema del bullismo dal titolo "Io non bullo", rivolto in particolare agli alunni delle classi prime e seconde.

Come già quest'anno, saranno previsti anche per il futuro incontri online o in presenza di soggetti esterni impegnati nel contrasto del fenomeno.

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).

Prevenzione e sensibilizzazione rappresentano le parole chiave nella lotta contro il fenomeno.

Di seguito sono elencate alcune azioni utili che il nostro Istituto intende perseguire in relazione a questa problematica:

- sensibilizzare gli studenti ad un uso sicuro e consapevole delle tecnologie digitali;
- adottare linee di orientamento per prevenire e contrastare il cyberbullismo anche con il supporto della Polizia postale nel controllo di quanto accade online;
- coinvolgere gli studenti in un percorso comune contro il fenomeno, anche mediante progetti anti-cyberbullismo;
- segnalare materiale inopportuno, abusi subiti o rilevati durante la navigazione in Internet o Social Network tramite i canali e gli strumenti offerti dal servizio al fine di ottenere la rimozione del contenuto;
- intervenire preventivamente al fine di evitare, arginare ed eliminare possibili manifestazioni di comportamenti antisociali;
- garantire la presenza a scuola di un referente per il bullismo e cyberbullismo;
- promuovere la sicurezza in Rete degli studenti affinché acquisiscano le competenze necessarie all'esercizio di una cittadinanza digitale consapevole;
- supportare alunni e famiglie in momenti di difficoltà;
- valutare i comportamenti che sfociano in disagio sociale, con la possibilità di coinvolgere anche un servizio specialistico socio-sanitario;
- attivare un'efficace integrazione con la rete dei servizi territoriali locali (Polizia postale, Questura, ASL etc...).

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.

Si intende:

- educare ad un uso etico e consapevole delle parole soprattutto in rete;
- Valorizzare la dimensione relazionale sensibilizzando gli adolescenti verso capacità di analisi che li aiutino a demolire gli stereotipi su cui spesso si fondano forme di hate speech, in particolare legati alla razza, al genere, all’orientamento sessuale, alla disabilità.

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?

In relazione a tale problematica e ai rischi che comporta l’iper-connessione, il nostro Istituto si propone di:

- promuovere azioni di prevenzione attraverso percorsi sul “benessere digitale”, ossia la capacità di sfruttare i vantaggi forniti dalla tecnologia mantenendo con essa una relazione sana ed equilibrata;
- incentivare attività di aggregazione;
- condividere momenti di riflessione con gli studenti su un uso consapevole delle TIC;
- seguire regole chiare e condivise durante la navigazione in Rete.

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.

In relazione al sexting, il nostro Istituto intende perseguire le azioni di seguito elencate:

- organizzare incontri, aperti anche ai genitori, con psicologi, esperti di diritto al fine di informare sui rischi penali in cui si può incorrere in seguito alla diffusione, anche inconsapevole, di immagini dal contenuto sessualmente esplicito;
- promuovere percorsi di Educazione civica per sensibilizzare ai problemi derivanti dal sexting.

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.

L'impatto della pandemia da Covid-19 sull'aumento dell'utilizzo delle tecnologie è stato evidente: ne ha ampliato l'uso ed ha abbassato ulteriormente la fascia d'età di chi accede ad ambienti digitali, ma ciò è avvenuto in modo repentino ed emergenziale, in assenza di un'adeguata preparazione.

Ai vantaggi dell'innovazione digitale si affianca anche l'esposizione a rischi specifici e, pertanto, è fondamentale prestare molta attenzione al fenomeno dell'adescamento online, purtroppo in costante diffusione.

È essenziale che gli insegnanti siano in grado di promuovere un utilizzo consapevole e critico della Rete e informare sui rischi in cui si può incorrere durante la navigazione. Far comprendere che alcuni comportamenti illeciti nel mondo reale lo sono anche in Rete.

È indispensabile accertare le conoscenze degli studenti ed eventualmente organizzare con loro una breve formazione per istruirli su temi quali la protezione della privacy, la gestione dell'immagine e dell'identità online.

È importante, inoltre, che gli alunni sappiano a chi rivolgersi in caso di problemi. Se si sospetta o si ha la certezza di un caso di adescamento online bisogna richiedere il prima possibile l'intervento della Polizia Postale tenendo presente che, trattandosi di una tematica molto delicata da gestire con possibili ripercussioni psicologiche significative sul minore, potrebbe essere necessario rivolgersi ad un Servizio territoriale (Consultorio Familiare, Servizio di Neuropsichiatria Infantile, ecc.) in grado di fornire alla vittima anche un adeguato supporto di tipo psicologico.

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.

Per quanto riguarda la pedopornografia è fondamentale, da un lato, un miglioramento del rapporto e del dialogo genitori-figli affinché si insaturi un clima di fiducia e, dall'altro, un sempre maggior coinvolgimento degli insegnanti e degli educatori nell'attività di prevenzione dei reati di adescamento dei minori via internet.

È necessario che l'Istituto diffonda e spieghi il contenuto delle norme proposte nelle leggi che si occupano di pedopornografia, avvalendosi di organi investigativi (magistrati, forze dell'ordine, polizia postale) coinvolgendo tutti gli attori della comunità scolastica, in primis le famiglie, affinché possano vigilare sulla diffusione online di comportamenti sessualmente espliciti nei dispositivi tecnologici dei propri figli.

Il nostro piano d'azioni

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

- 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.
- Promuovere incontri e laboratori per studenti e studentesse dedicati all' Educazione Civica Digitale.

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

- Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse.
- 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.

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.

Pertanto sono da considerare degni di segnalazione:

- contenuti afferenti la violazione della privacy (foto personali, l'indirizzo di casa o il telefono, informazioni private proprie o di amici, foto o video pubblicati contro la propria volontà, di eventi privati, ecc.);
- contenuti afferenti all'aggressività o alla violenza (messaggi minacciosi, commenti offensivi, pettegolezzi, informazioni false, foto o video imbarazzanti, virus, contenuti razzisti, che inneggiano al suicidio, immagini o video umilianti, insulti, videogiochi pensati per un pubblico adulto, ecc.);
- contenuti afferenti alla sessualità: messaggi molesti, conversazioni (testo o voce) che connotano una relazione intima e/o sessualizzata, foto o video personali con nudità o abbigliamento succinto, immagini pornografiche, foto e video in cui persone di minore età sono coinvolte o assistono ad attività sessuali (pedopornografia), ecc.

I docenti, in particolare, sono chiamati a essere spazio di avamposto privilegiato nella gestione delle problematiche, dei rischi, dei pericoli che gli adolescenti possono vivere e affrontare ogni giorno.

Accorgersi tempestivamente di quanto accade e compiere azioni immediate di contrasto verso gli atti inopportuni -quando non illegali- diviene fondamentale per poter evitare conseguenze a lungo termine che possano pregiudicare il benessere e una crescita armonica dei soggetti coinvolti.

Per poter rilevare i casi acuti o di emergenza la scuola attiva un sistema di segnalazione tempestiva e una valutazione approfondita in funzione della gravità del problema, attraverso quattro specifici passaggi:

1. raccolta della segnalazione e presa in carico del caso;

2. approfondimento della situazione per definire il fenomeno;

3. gestione del caso con scelta dell'intervento o degli interventi più adeguati da attuare (individuale, educativo con il gruppo classe, di mantenimento e ripristino della relazione, intensivo e a lungo termine, di coinvolgimento delle famiglie);

4. monitoraggio della situazione e dell'efficacia degli interventi.

Al fine di meglio regolamentare l'insieme dei provvedimenti sia di natura disciplinare che di natura educativa e di prevenzione da mettere in campo in tali circostanze, le misure di intervento immediato che il Dirigente è chiamato a effettuare, qualora venga a conoscenza di episodi di cyberbullismo, sono integrate e previste nel Regolamento di

Istituto e nel Patto di corresponsabilità.

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.

Le studentesse e gli studenti possono segnalare in anonimato episodi di bullismo e/o cyberbullismo direttamente inquadrando un QRCode.

Sarà data inoltre ampia comunicazione della possibilità, per studentesse e gli studenti, di rivolgersi alla Helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

Per quanto riguarda la gestione dei casi, il nostro Istituto ha individuato una figura referente per il bullismo e il cyberbullismo e la costituzione di un Team Antibullismo composto dal Dirigente scolastico, dal referente per il bullismo e cyberbullismo, dalle funzioni strumentali di area pertinente, dall'animatore digitale.

La segnalazione del caso dovrà essere fatta dal singolo docente, alla referente, la quale, insieme al Team Antibullismo, si occuperà di raccogliere tutte le informazioni possibili, anche attraverso colloqui di approfondimento con gli attori coinvolti e di segnalare l'accaduto al Dirigente.

Sarà poi il Dirigente, insieme al Team, a valutare se la segnalazione debba essere rivolta ad organi esterni alla scuola quali la Polizia Postale o i Servizi Sociali o se il caso vada gestito all'interno della scuola con il coinvolgimento del Consiglio di Classe e delle famiglie degli alunni coinvolti.

Le procedure interne da attivare per la gestione di casi sospetti o evidenti di bullismo e/o cyberbullismo sono riportate in allegato al presente documento.

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.

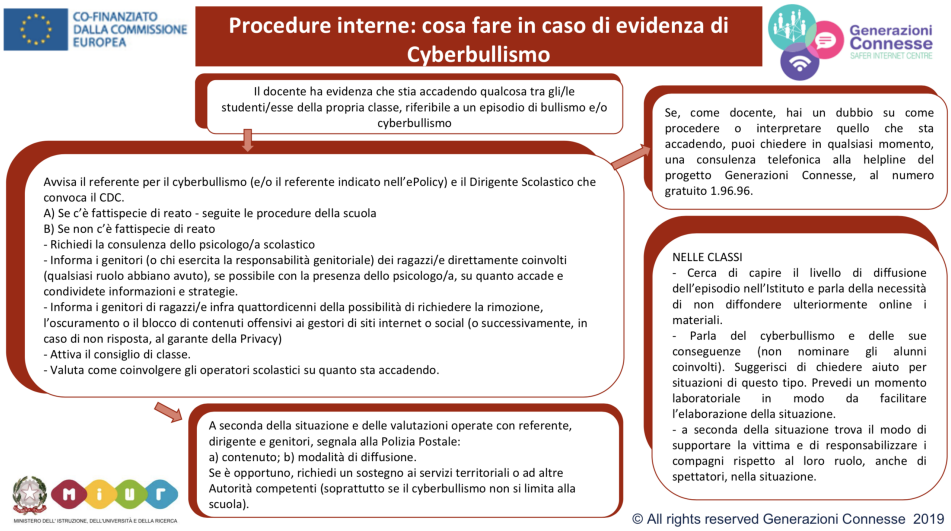
A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti

che una problematica connessa all'utilizzo di Internet può presentare.

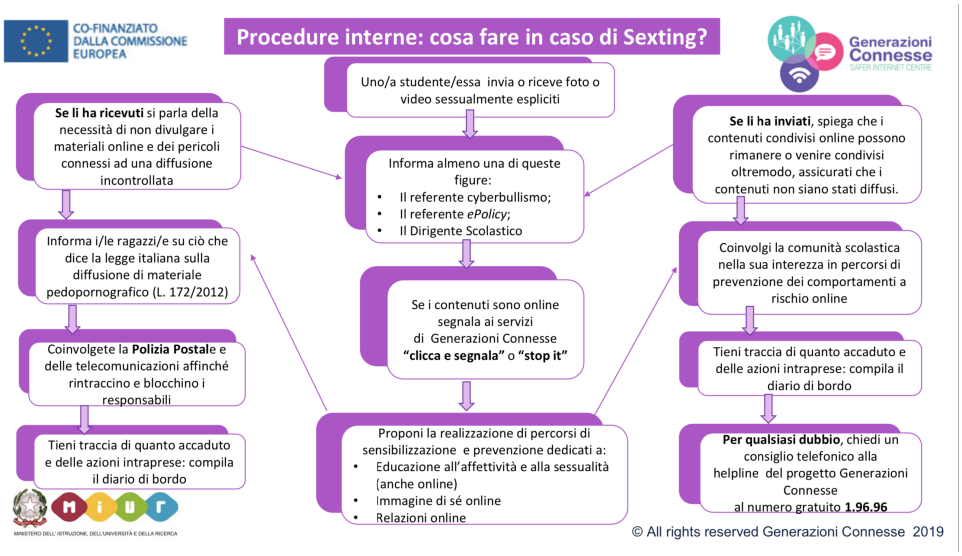
- **Comitato Regionale Unicef**: laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni)**: svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare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

5.4. - Allegati con le procedure

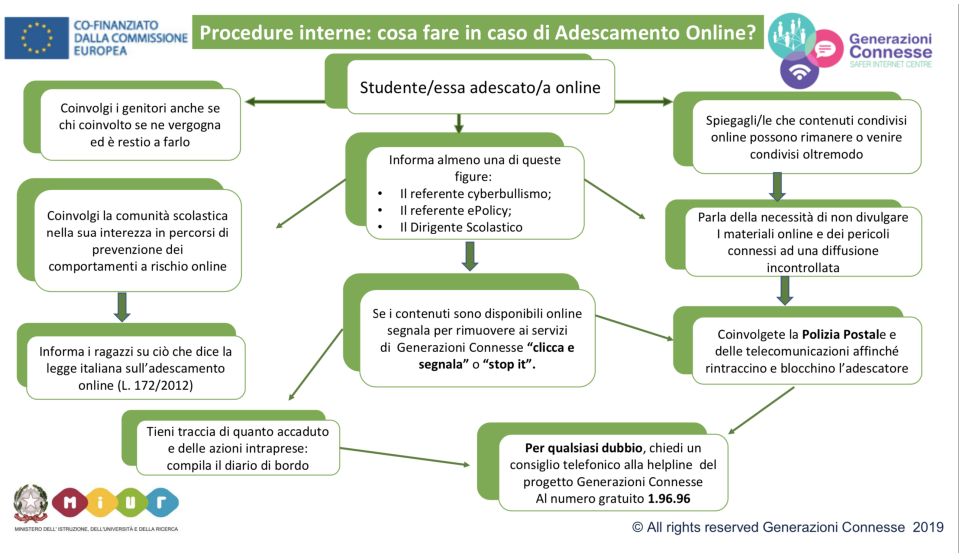
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



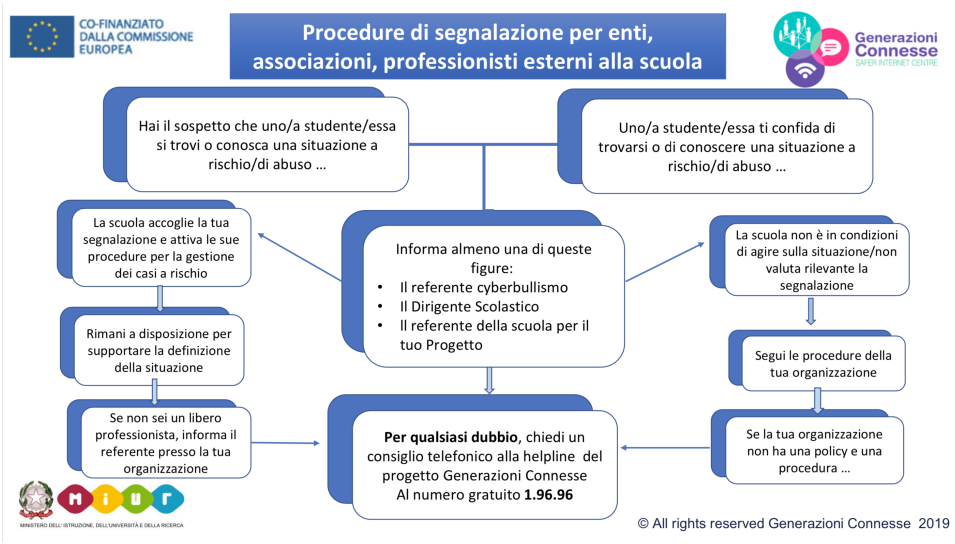
Procedure interne: cosa fare in caso di sexting?



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

Non è prevista nessuna azione.