ISTITUTO COMPRENSIVO ARBE ZARA
C.F. 80124730153 C.M. MIIC8DG00L
AR90809 - IC ARBE ZARA
Prot. 0003453/U del 08/07/2025

FUTURA LA SCUOLA PER L'ITALIA DI DOMANI

Finanziato dall'Unione europea NextGenerationEU

Ministero dell'Istruzione e del Merito

Italiadomani

Istituto comprensivo "Arbe - Zara"

Viale Zara n. 96 (via Arbe, 21) - 20125 MILANO
C.F. 80124730153 – Cod. Mecc. MIIC8DG00L
Milano ☎ 02/88467600
Sito Istituto: www.icarbezara.edu.it - posta istituzionale: MIIC8DG00L@istruzione.it
posta certificata: MIIC8DG00L@pec.istruzione.it
Codice univoco per fatturazione elettronica **UF58DE**

Documento di ePolicy

Capitolo 1 INTRODUZIONE AL DOCUMENTO EPOLICY

1.1 - Scopo dell'ePolicy

1.2 – Perché è importante dotarsi di un ePolicy?

1.3 - Ruoli e responsabilità

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

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

1.6 - Gestione delle infrazioni all'ePolicy

1.7 - Integrazione dell'ePolicy con regolamenti esistenti

1.8 - Monitoraggio dell'implementazione dell'ePolicy e suo aggiornamento

Capitolo 2 FORMAZIONE e CURRICOLO

2.1 - Curricolo sulle competenze digitali per gli studenti

2.2 - Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie 2.3 - dell'Informazione e della Comunicazione) nella didattica

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

2.4 - Sensibilizzazione delle famiglie

Capitolo 3 GESTIONE DELL'INFRASTRUTTURA E DELLA STRUMENTAZIONE ICT DELLA E NELLA SCUOLA

3.1 - Protezione dei dati personali

3.2 - Accesso ad Internet

3.3 - Strumenti di comunicazione online

3.4 - Strumentazione personale

Capitolo 4. RISCHI ONLINE: CONOSCERE, PREVENIRE E RILEVARE

4.1 - Sensibilizzazione e prevenzione

4.2 - Cyberbullismo: che cos'è e come prevenirlo

4.3 - Dipendenza da Internet e gioco online

4.4 - Hate speech: che cos'è e come prevenirlo

4.5 - Sexting

4.6 - Adescamento online

4.7 - Pedopornografia

Capitolo 5. SEGNALAZIONE E GESTIONE DEI CASI

5.1 - Cosa segnalare

5.2 - Come segnalare: quali strumenti e a chi

5.3 - Gli attori sul territorio per intervenire

Capitolo 6 ALLEGATO CON PROCEDURE

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

6.2 - Procedure interne: cosa fare in caso di sexting?

6.3 - Procedure interne: cosa fare in caso di adescamento online?

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

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.

1.2 - Perché è importante dotarsi di un ePolicy?

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.

Finalità del presente documento è regolamentare in modo organico e condiviso dall'intera Comunità Scolastica i comportamenti e le procedure in merito all'utilizzo delle Tecnologie dell'Informazione e della Comunicazione (TIC) nella didattica, promuoverne un uso critico e consapevole, prevenire, rilevare, gestire e contrastare le problematiche derivanti da un uso ignaro ed improprio delle tecnologie digitali.

Il Piano Nazionale Scuola Digitale affida esplicitamente alla scuola il compito di rafforzare le competenze digitali per consentire ai cittadini di domani di esercitare pienamente i loro diritti e di abitare in maniera consapevole il mondo sempre più "glocale". Il nostro Istituto riconosce come le TIC rappresentino una grande opportunità per sostenere l'insegnamento, promuovere la creatività, stimolare la consapevolezza e migliorare l'apprendimento degli studenti, ma è conscio dei rischi relativi e della conseguente necessità di fronteggiarli adeguatamente.

Il nostro Istituto, con questa E-policy, ha deciso di adottare una politica di prevenzione attraverso:

- La messa in campo di azioni informative e di confronto volte al riconoscimento precoce di comportamenti a rischio con lo scopo di intervenire prima della possibile insorgenza di fenomeni veri e propri di bullismo e /o cyberbullismo, azioni che possano promuovere l'uso consapevole e funzionale delle tecnologie e dei social.

- La promozione di interventi educativi e azioni a supporto di studenti e studentesse vittime di cyberbullismo o di problematiche relative all'utilizzo della rete, in linea con la legge 71/2017 "Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo".

- Realizzazione di interventi con la Funzione Strumentale nelle classi prime della Scuola Secondaria di primo grado, sia per sensibilizzare gli studenti sui temi del bullismo e del cyberbullismo, sia per sollecitare una riflessione su questi argomenti e fare uno screening preventivo di eventuali criticità

- Incontri con esperti per rafforzare il tema del bullismo e cyberbullismo con famiglie e studenti

1.3 - 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 appartenente alla comunità educante nel momento in cui utilizza la rete deve:

- Rispettare il presente documento e la normativa vigente;
- Tutelare la privacy di tutti gli utenti coinvolti;
- Rispettare la "netiquette", galateo della rete.

All'interno della comunità educante ogni figura ha un ruolo specifico.

Il Dirigente Scolastico deve:

- Promuovere l'uso consapevole delle tecnologie e di internet garantendo la sicurezza, anche online, di tutti i membri della comunità scolastica, in linea con il quadro normativo di riferimento e le indicazioni del MIUR;
- Promuovere la sicurezza online dando il proprio contributo all'organizzazione, insieme al TIM prevenzione bullismo/cyberbullismo, di corsi di formazione specifici per tutte le figure scolastiche, sull' utilizzo positivo e responsabile delle TIC.
- In caso di episodi manifesti di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali ha il compito di intervenire sia sul piano educativo che sanzionatori.

DS con DSGA (GESTORI DATI E INFORMAZIONI devono:

- Assicurare nei limiti delle risorse finanziarie disponibili l'intervento di tecnici per garantire che l'infrastruttura tecnologica della scuola sia funzionante, sicura, non aperta ad uso improprio o a dannosi attacchi esterni;
- Favorire il funzionamento dei diversi canali di comunicazione all'interno della scuola e fra la scuola e le famiglie;
- Garantire che i dati di gestione siano accurati e aggiornati;
- Promuovere le migliori pratiche nella gestione delle informazioni, ossia mettere in atto un sistema di controllo di accesso appropriato. I dati sono utilizzati, trasferiti e cancellati in linea con i requisiti di protezione dei dati;

- Mantenere i controlli di accesso per proteggere le informazioni sensibili archiviati su dispositivi di proprietà della scuola.

L'Animatore digitale ha il compito di:

- Promuovere corsi di formazione d'Istituto sulle TIC, supportare il personale scolastico sia dal punto di vista tecnico e informatico sia in merito alla tutela della privacy.

- Monitorare e rilevare eventuali episodi o problematiche connesse all'uso delle TIC a scuola controllando che tutti gli utenti autorizzati accedano alla Rete della scuola con apposita password, per scopi istituzionali e consentiti (istruzione e formazione).

Il Referente bullismo e cyberbullismo ha il compito di:

- Coordinare e promuovere azioni specifiche per la prevenzione e il contrasto del fenomeno del bullismo e del cyberbullismo. La scuola può avvalersi della collaborazione delle Istituzioni, delle Forze di polizia, delle associazioni e dei centri di aggregazione giovanile del territorio.

- Il team prevenzione bullismo e cyberbullismo può coinvolgere in progetti e percorsi formativi tutta la comunità educante.

I Docenti hanno il compito di:

- Diffondere la cultura dell'uso responsabile e consapevole delle TIC e della Rete. Possono utilizzare le TIC nella didattica della propria disciplina per offrire ai ragazzi più strumenti mettendo così tutti i ragazzi nelle condizioni di poterli utilizzare senza mettere in "risalto" gli alunni con BES. I docenti devono supportare gli studenti nelle attività di apprendimento e nei laboratori che prevedono l'uso della LIM o di altri dispositivi tecnologici connessi in Rete.

- Educare gli studenti all'importanza del rispetto della privacy ricordando loro di segnalare sempre eventuali siti che possono spaventare o comunicare ai genitori di aver conosciuto persone online. È importante che gli alunni siano informati sui rischi presenti in Rete, vanno educati ad un uso consapevole in modo che Internet possa essere per i ragazzi una fonte di divertimento oltre che un utile strumento di apprendimento.

- I docenti devono osservare i comportamenti a rischio dei ragazzi e hanno il dovere morale e professionale di segnalare al Dirigente Scolastico che insieme al Referente per il Cyberbullismo e al Consiglio di Classe potrà definire strategie di intervento

condivise.

Personale ATA deve:

- Segnalare comportamenti non adeguati e/o episodi di bullismo/cyberbullismo.

Gli Studenti e le Studentesse devono:

- Mostrare di saper utilizzare in modo consapevole le tecnologie digitali in coerenza con quanto richiesto dai docenti. Con il supporto della scuola devono partecipare ai progetti e alle attività proposte sull'utilizzo consapevole delle TIC dovrebbero imparare a tutelarsi online, potrebbero inoltre promuovere percorsi di peer education per aiutare i compagni più piccoli in questo percorso di crescita favorendo una continuità verticale che è molto a cuore al nostro Istituto.

I Genitori hanno il compito di:

- collaborare con l'Istituto scolastico, sono attori partecipi e attivi nelle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete, nonché sull'uso responsabile dei device personali. Come parte della comunità educante sono tenuti a relazionarsi con i docenti sulle linee educative che riguardano le TIC e la Rete e hanno il dovere di confrontarsi con loro nel momento in cui rilevano che i propri figli fanno un uso scorretto e poco responsabile delle tecnologie digitali o di Internet. È importante che accettino e condividano quanto scritto nell'ePolicy dell'Istituto e nel patto di responsabilità in un'ottica di collaborazione reciproca. Bisogna, inoltre, ricordare che esiste una corresponsabilità educativa e formativa che riguarda sia i genitori che la scuola nel percorso di crescita degli studenti e delle studentesse.

1.4 - 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).

Tutti gli operatori esterni presenti a qualsiasi titolo nella scuola dovranno attenersi alle norme previste dal presente documento di e-Policy dell'Istituto.

Nella realizzazione di progetti, le collaborazioni con enti o figure esterne devono essere preventivamente concordate con il TEAM prevenzione bullismo e cyberbullismo e autorizzate dal Dirigente scolastico.

1.5 - 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, una volta approvato dal Collegio dei Docenti e dal Consiglio di Istituto sarà 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 verranno 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.

1.6 - Gestione delle infrazioni all'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 sanzioni, riferite soprattutto agli alunni, avranno come carattere preferenziale quello educativo/riabilitativo e in ogni caso verrà coinvolta la componente genitori, in qualità di primi educatori.

Le infrazioni saranno riferite direttamente al Dirigente Scolastico che provvederà a convocare un Consiglio di Classe straordinario nel quale si decideranno le azioni da intraprendere, facendo riferimento al Regolamento Disciplinare d'Istituto.

Tali provvedimenti, che avranno carattere educativo e possibilmente non punitivo, saranno indirizzati in parte al soggetto che ha compiuto l'infrazione e in parte al gruppo classe in cui è inserito; si ritiene, infatti, che l'azione educativa verso il singolo assuma forza e valenza solo se si crea uno spazio di ascolto e di riflessione di gruppo e un'occasione per il reciproco aiuto.

1.7 - Integrazione dell'ePolicy con regolamenti esistenti

Il Regolamento dell'Istituto Scolastico viene aggiornato con specifici riferimenti all'E policy, così come anche il Patto di Corresponsabilità, in coerenza con le Linee Guida Miur e le indicazioni normative generali sui temi in oggetto.

La e-Policy dell'I.C Arbe Zara fa riferimento e si armonizza con tutti gli altri regolamenti vigenti nell'Istituto, in particolare con PTOF, Regolamento interno e Patto di Corresponsabilità Educativa

1.8 - Monitoraggio dell'implementazione dell'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 e-Policy verrà curato dai docenti referenti e da uno specifico gruppo di lavoro che si riunirà per incontri e confronti, al fine di discutere di prevenzione, di visionare materiali, aderire a progetti relativi alla sicurezza in Rete e qualora si verifichino cambiamenti significativi in riferimento all'uso delle tecnologie digitali all' interno della scuola, per rivedere, modificare e/o ampliare la e-Policy, in una logica di condivisione con tutto il corpo docente, il Dirigente Scolastico, la Funzione Strumentale per il PTOF e le famiglie.

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.

La competenza digitale, per la sua importanza nelle attività professionali e anche quotidiane, è ritenuta dall'Unione Europea una competenza chiave per lo sviluppo del senso di cittadinanza. Nel curricolo disciplinare del nostro Istituto tale competenza pervade in modo trasversale i vari insegnamenti; questa declinazione scaturisce dalla necessità di iniziare a dare una formazione di base sull'uso delle TIC, inserendole nelle attività didattiche, per arrivare nelle classi finali a fornire gli strumenti per un approccio consapevole, critico, autonomo e responsabile.

Negli ultimi anni la scuola ha provveduto all'implementazione della dotazione digitale dei vari plessi, anche attraverso la partecipazione ai progetti, per consentire l'introduzione di metodologie basate sull'uso delle TIC.

2.2 - Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie 2.3 - 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.

Pertanto l'I.C Arbe Zara propone di consolidare le competenze digitali del personale docente, anche attraverso momenti di formazione interna, da erogare in presenza o in modalità a distanza.

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.

2.4 - Sensibilizzazione delle famiglie

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"

L'Istituto ha promosso e continua a promuovere iniziative per sensibilizzare le famiglie all'uso consapevole delle TIC e della rete, promuovendo la conoscenza delle numerose situazioni di rischio online. A tal fine sono previsti incontri fra genitori e specialisti per la diffusione del materiale informativo su queste tematiche. Saranno favoriti momenti di confronto e discussione anche sulle dinamiche che potrebbero instaurarsi fra i pari con l'uso di cellulari e

smartphone o del chat-line o social network più diffusi, con particolare riferimento alla prevenzione del cyberbullismo.

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 il 19 settembre 2018.

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.

Sono dati personali le informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, etc. La nostra scuola è impegnata in prima persona nella tutela della privacy degli utenti attraverso l'applicazione del regolamento d'Istituto e del patto di corresponsabilità.

Nella scuola la responsabilità del trattamento dei dati personali dell'Istituzione scolastica, è esercitata dal Dirigente Scolastico.

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.

Tutti i plessi dell'Istituto sono dotati di una rete wireless alla quale sono connessi la maggior parte dei dispositivi; ove possibile e conveniente (per es. laboratori di informatica) si procede alla connessione alla rete internet attraverso cavo.

I dispositivi sono collegabili alla rete internet esclusivamente tramite password. Si ritiene utile che il personale docente di ogni plesso, o almeno un rappresentante di essi, sia a conoscenza della password di accesso, così da poter connettere facilmente tutti i dispositivi necessari per lo svolgimento delle attività didattiche.

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.

Il personale interno alla scuola (D.S., docenti, personale di segreteria) e i genitori hanno a disposizione la mail istituzionale per le comunicazioni "interne".

Il sito web della scuola (https://icarbezara.edu.it/) è la prima e principale interfaccia dell'Istituto. Oltre alle informazioni generali e di contatto, vi si trovano apposite sezioni dedicate alle Scuole, ai Servizi, alla Didattica ai Progetti nonché fondamentali comunicazioni, informazioni, modulistica per docenti, personale ATA alunni e famiglie.

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.

La presente ePolicy contiene un Regolamento è fondamentale per garantire un ambiente educativo sicuro, rispettoso e favorevole all'apprendimento.

Il nostro regolamento stabilisce che:

Gli studenti si impegnano a:

➔ Mantenere spento il cellulare, il tablet o lo smartwatch durante tutto l'orario scolastico,

inclusi i momenti di pausa, mensa, attività organizzate dalla scuola sul territorio o visite guidate;

➔ Conservare i dispositivi spenti in cartella;

➔ Utilizzare il cellulare solamente al termine delle lezioni e al di fuori dell'edificio scolastico;

➔ Utilizzare il proprio dispositivo digitale per scopi didattici, solo se espressamente richiesto dal/la docente e conformemente alle indicazioni e agli orari da lui/lei stabiliti.

Durante le uscite didattiche di una o più giornate:

Primaria:

➔ Gli studenti della Primaria non sono autorizzati a portare con sé il cellulare o il tablet, nemmeno senza SIM per fare foto; Il docente di classe si terrà in contatto con un rappresentante dei genitori per dare notizie sull'andamento dell'uscita didattica. Il rappresentante di classe informerà poi a sua volta tutti gli altri genitori.

Secondaria:

➔ Durante le uscite di una o più giornate in Italia con pernottamento presso una struttura ricettiva, il cellulare non può essere utilizzato durante gli spostamenti in pullman/treno e deve rimanere spento nello zaino;

➔ Durante il soggiorno, gli studenti dovranno consegnare il cellulare ai docenti all’orario

stabilito di volta in volta in base alle esigenze del momento. Gli insegnanti lo restituiranno solo dopo cena per un periodo limitato di tempo, al fine di consentire la comunicazione con le famiglie. Successivamente, il cellulare verrà nuovamente consegnato ai docenti per garantire un riposo notturno tranquillo;

➔ Il docente accompagnatore si assicurerà di aggiornare quotidianamente un rappresentante dei genitori sull'andamento dell'uscita didattica, il quale informerà gli altri genitori.

➔ Nel caso di uscite all'estero con alloggio presso una famiglia ospite, di norma, viene consentito l'utilizzo del cellulare, al fine di mantenere un costante contatto con i propri docenti. Tuttavia, durante il viaggio e le attività didattiche, si applicano le stesse regole stabilite per le normali attività a scuola, come descritto precedentemente.

Le regole sopra descritte possono essere modificate o adattate dai docenti accompagnatori in base alle specifiche necessità dell'uscita didattica e alle situazioni particolari che si manifestano di volta in volta.

I <u>docenti</u> si impegnano a:

➔ Non utilizzare il cellulare durante le ore di servizio per scopi non correlati alla loro funzione docente e istituzionale;

I <u>genitori</u>:

➔ Non possono diffondere al di fuori dell'ambito scolastico immagini o video realizzati personalmente o scaricati dai canali ufficiali della scuola che rappresentano momenti di attività didattica, con la presenza di studenti e/o insegnanti (come spettacoli natalizi, eventi sportivi o uscite didattiche

Capitolo 4. RISCHI ONLINE: 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 sé stessi o altri;
- essere una vittima di queste azioni;
- osservare altri commettere queste azioni.

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

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

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

La necessità di sensibilizzare ad un uso positivo e consapevole delle TIC gli studenti e le studentesse, sia in un'ottica di tutela dai rischi potenziali che di valorizzazione delle opportunità esistenti, pone la scuola ed i genitori di fronte alla sfida di riconsiderare la propria identità, il proprio ruolo educativo e le proprie risorse, oltre allo stato dei rapporti reciproci per un patto educativo da rinnovare costantemente. Tra le misure di prevenzione che la scuola mette in atto ci sono azioni finalizzate a promuovere una cultura dell'inclusione, del rispetto dell'altro/a e delle differenze così che l'utilizzo di Internet e dei cellulari oltre che collocarci all'interno di un sistema di relazioni, ci renda consapevoli di gestire con un certo grado di lucidità i rapporti che si sviluppano in tale ambiente, giungendo a riconoscere e gestire le

proprie emozioni.

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;
- Coadiuva il Dirigente scolastico nella redazione dei Piani di vigilanza attiva ai fini della prevenzione degli episodi di bullismo e di cyberbullismo;

- Monitora i casi di bullismo e cyberbullismo, coordina il Team Antibullismo, crea alleanze con il Referente territoriale e regionale, coinvolge in un'azione di collaborazione Enti del territorio in rete (psicologi, forze dell'ordine, assistenti sociali, pedagogisti, ecc.)

4.3 - 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 forma i ragazzi affinché l'uso della rete sia sempre sereno e consapevole, in modo da favorire il benessere digitale dei ragazzi stessi. Qualora si riscontrino casi che coinvolgano gli studenti dell'Istituto in accordo con le famiglie saranno proposti eventuali percorsi educativi e/o di supporto psicologico ad opera di personale specializzato.

4.4 - 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.

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.

Il nostro Istituto propone nelle classi terze della Scuola secondaria di I grado percorsi di **educazione all'affettività e alla sessualità** al fine di rendere le alunne e gli alunni più sicuri emotivamente e pronti ad affrontare eventuali situazioni a rischio, imparando innanzitutto a gestire le proprie emozioni, il rapporto con il proprio corpo e con gli altri.

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).

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.

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.

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.

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.

A seguito della messa in atto di azioni preventive, nel caso si verificassero comportamenti a rischio, il docente che ne venisse a conoscenza deve adoperarsi per mettere al corrente dell'accaduto il Dirigente, il Consiglio di classe e la famiglia, affinché si possano trovare azioni di contrasto efficaci e mirate a moderare gli effetti o eliminarli.

Nel caso si trattasse di fenomeni di cyberbullismo, verrà contattato il referente scolastico per il Cyberbullismo.

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.

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.

Si considerano da segnalare tutte quelle situazioni caratterizzate da volontarie e ripetute aggressioni mirate a insultare, minacciare, diffamare e/o ferire una persona o un piccolo gruppo tramite un utilizzo irresponsabile dei Social Network. in particolare si segnaleranno:

- contenuti afferenti la violazione della privacy (foto personali, indirizzo di casa o il telefono, informazioni private proprie o di amici, foto, 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 o umilianti, virus, contenuti razzisti,

che inneggiano al suicidio, insulti, videogiochi pensati per un pubblico adulto, hate speech, 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 o video in cui minori sono coinvolti o assistono ad atti sessuali (pedopornografia) ecc.

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 studenti 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 studenti della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.

Gli alunni possono effettuare personalmente le loro segnalazioni a qualunque docente dell'Istituto. I genitori possono effettuare le loro segnalazioni personalmente ai docenti di classe, al responsabile per il cyberbullismo o al Dirigente Scolastico. I docenti sono tenuti ad effettuare le segnalazioni al DS, a coinvolgere il Consiglio di classe e il referente per il cyberbullismo. Il Dirigente scolastico, monitorata la situazione, potrà eventualmente allertare gli operatori dei Servizi Sociali o di polizia laddove sia necessario.

La scuola mette a disposizione di studenti e studentesse i seguenti strumenti di segnalazione:

1. Indirizzi mail istituzionali dei docenti per segnalazioni da parte degli studenti e delle studentesse;

2. Docente referente per le segnalazioni (Coordinatore di plesso);

3. Sportello di ascolto con lo psicologo della scuola.

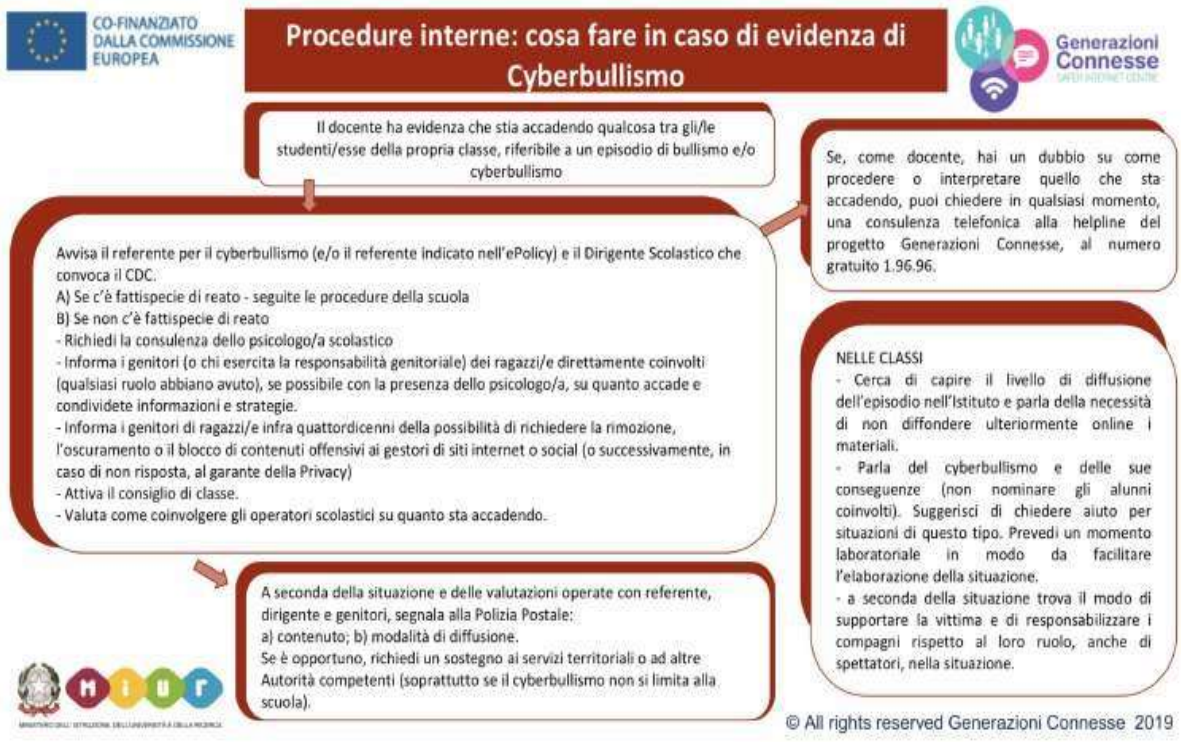
5.3 - Gli attori sul territorio per intervenire

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.

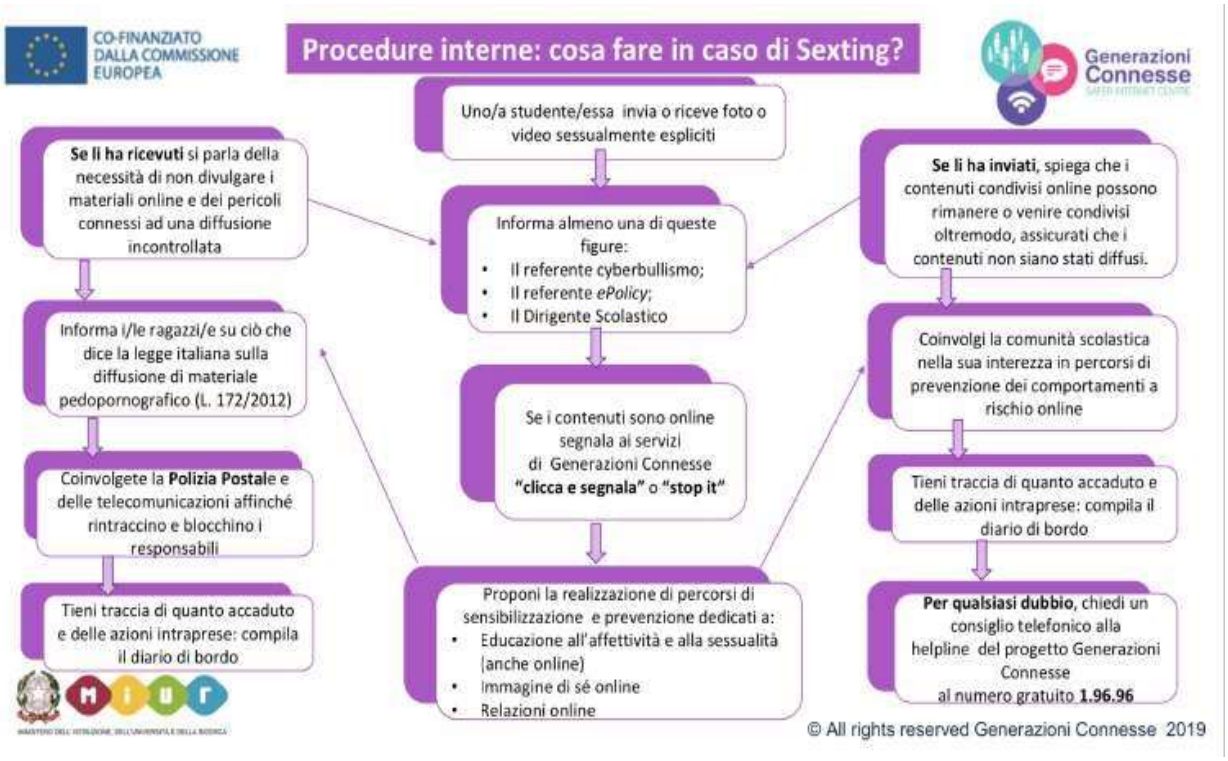
La scuola, dopo un confronto interno ed il confronto con i genitori e lo psicologo della scuola, si rivolgerà ai Servizi Sociali del territorio e se necessario, alle Forze dell'Ordine.

Capitolo 6 ALLEGATI CON PROCEDURE

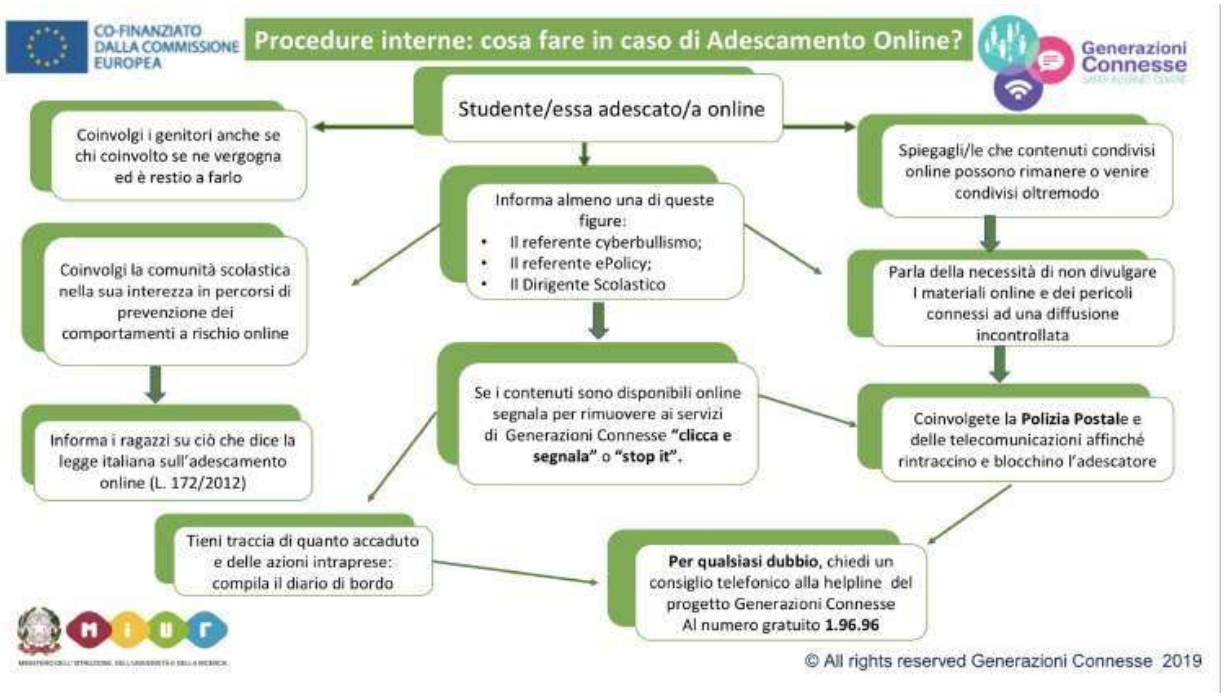
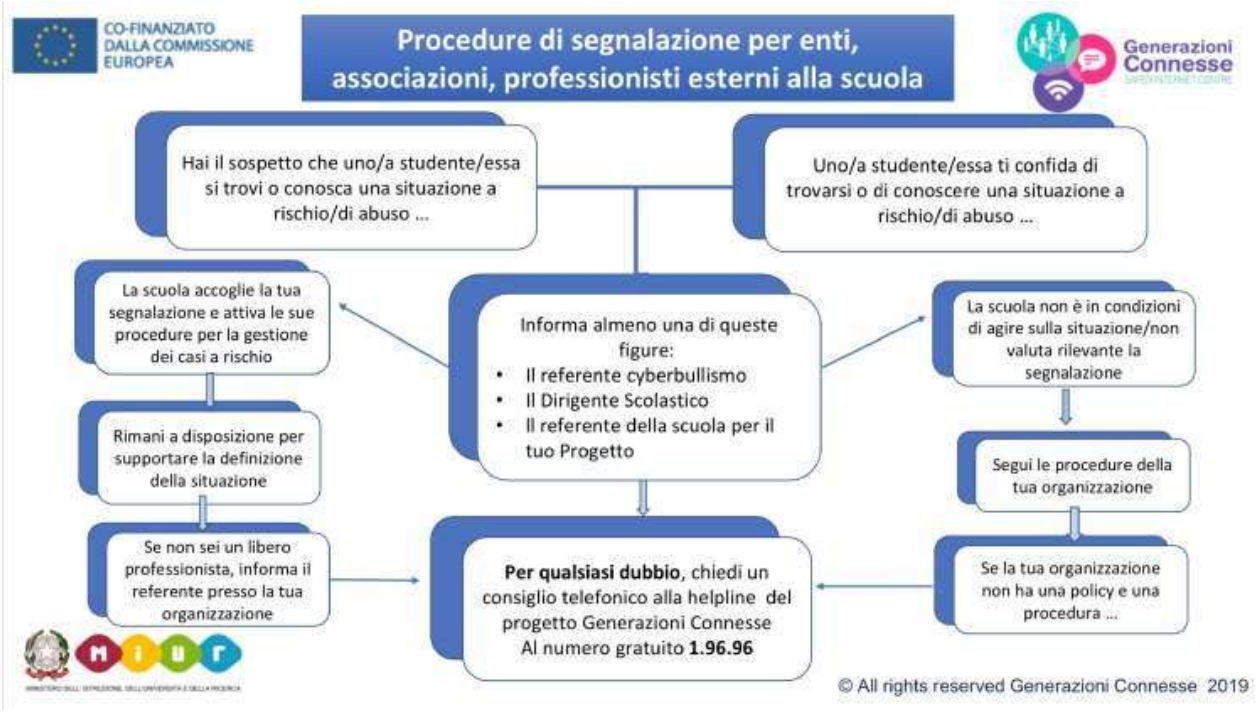
6.1 - Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



6.2 - Procedure interne: cosa fare in caso di sexting?



6.3 - Procedure interne: cosa fare in caso di adescamento online?



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