Documento di ePolicy

ANIC850006

I. C. "RITA LEVI-MONTALCINI"

VIA PAGANINI 5 - 60033 - CHIARAVALLE - ANCONA (AN)

Lorenzo Savini

Documento informatico firmato digitalmente da Lorenzo Savini ai sensi del D.Lgs 82/2005 s.m.i. e norme collegate

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

1. **Presentazione dell'ePolicy**
    1. Scopo dell'ePolicy
    2. Ruoli e responsabilità
    3. Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto
    4. Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica
    5. Gestione delle infrazioni alla ePolicy
    6. Integrazione dell'ePolicy con regolamenti esistenti
    7. Monitoraggio dell'implementazione dell'ePolicy e suo aggiornamento
2. **Formazione e curricolo**
    1. Curricolo sulle competenze digitali per gli studenti
    2. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica
    3. Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali
    4. Sensibilizzazione delle famiglie e Patto di corresponsabilità
3. **Gestione dell'infrastruttura e della strumentazione ICT (Information and Communication Technology) della e nella scuola**
    1. Protezione dei dati personali
    2. Accesso ad Internet
    3. Strumenti di comunicazione online
    4. Strumentazione personale
4. **Rischi on line: conoscere, prevenire e rilevare**
    1. Sensibilizzazione e prevenzione
    2. Cyberbullismo: che cos'è e come prevenirlo
    3. Hate speech: che cos'è e come prevenirlo
    4. Dipendenza da Internet e gioco online
    5. Sexting
    6. Adescamento online
    7. Pedopornografia
5. **Segnalazione e gestione dei casi**
    1. Cosa segnalare
    2. Come segnalare: quali strumenti e a chi
    3. Gli attori sul territorio per intervenire
    4. Allegati con le procedure

Perché è importante dotarsi di una E-policy?

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

all'uso di Internet.

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

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.

Le figure professionali che nella nostra scuola si occupano di gestione e programmazione delle attività formative, didattiche ed educative dell'Istituto sono le seguenti:

Il Dirigente scolastico

- promuove l'aggiornamento dei Regolamenti di istituto, il Patto educativo di corresponsabilità, il Regolamento generale d'Istituto con il coinvolgimento degli Organi Collegiali;
- promuove nell'Istituto l'uso consapevole delle tecnologie e di internet mediante la formazione della comunità educante (genitori/tutori, docenti, personale ATA);
- cura la tutela degli aspetti legali riguardanti la privacy e l'immagine di tutti i membri della comunità scolastica;
- crea un team trasversale e verticale che si occupi di promuovere la formazione del cittadino digitale, attraverso l'uso corretto e responsabile delle TIC da parte di tutti gli attori;
- implementa un sistema di monitoraggio e di controllo interno della sicurezza online;
- interviene nei casi di bullismo e cyberbullismo in un'ottica educativa.

L’Animatore digitale

- coinvolge la comunità scolastica nella partecipazione a piattaforme, attività e progetti attinenti il PNSD;
- stimola la formazione interna all’istituzione negli ambiti di sviluppo della “scuola digitale” e fornisce consulenza e informazioni al personale, in relazione ai rischi on-line e alle misure di prevenzione e gestione degli stessi;
- organizza, inoltre, il monitoraggio e la rilevazione di eventuali episodi o problematiche connesse all’uso delle TIC e ha il compito di controllare che l'accesso alla Rete della scuola sia regolamentato nonché avvenga, secondo le modalità previste, per scopi istituzionali e consentiti (istruzione e formazione).

Il Referente bullismo e cyberbullismo

- collabora con il Dirigente scolastico nella gestione di bullismo e cyberbullismo;
- coordina e promuove iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo con particolare attenzione all’educazione alle LIFE SKILLS, all’affettività e alla sessualità;
- collabora in team con l’Animatore digitale, il gruppo ePolicy, il referente BES per l’inclusione e con lo Psicologo scolastico;
- mantiene i contatti con associazioni e agenzie educative del territorio. Fondamentale, dunque, il suo ruolo non solo in ambito scolastico ma anche in quello extrascolastico.
- coinvolge, con progetti e percorsi formativi ad hoc, studenti, colleghi e genitori.

Lo Psicologo scolastico

- supporta le iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo con particolare attenzione all'educazione alle LIFE SKILLS;
- collabora con il Dirigente scolastico e il Referente bullismo e cyberbullismo;
- gestisce il punto di ascolto psicologico.

I Docenti

- diffondono la cultura dell'uso responsabile delle TIC e della Rete, integrando parti del curriculum della propria disciplina con approfondimenti mirati che prevedono anche l'uso delle tecnologie digitali nella didattica;
- supportano gli alunni e le famiglie nell'uso consapevole delle tecnologie informatiche utilizzate a scopi didattici per informarli/formarli sin dalla scuola dell'infanzia;
- hanno il dovere morale e professionale di segnalare al Dirigente Scolastico qualunque problematica, violazione o abuso, anche online, che vede coinvolti studenti e studentesse;
- aderiscono alle iniziative formative organizzate dall'Istituto, relative all'utilizzo del digitale nella didattica con particolare riferimento alla dimensione etica (tutela della privacy, rispetto dei diritti intellettuali dei materiali reperiti in Internet e dell'immagine altrui, lotta al cyberbullismo);
- promuovono iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo con particolare attenzione all'educazione alle LIFE SKILLS, all'affettività e alla sessualità.

Il personale Amministrativo, Tecnico e Ausiliario (ATA)

- è coinvolto nell'applicazione del PNSD

- promuove un uso corretto dei dati nel rispetto della privacy
- è coinvolto nella gestione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo.

Gli Studenti e le Studentesse

- utilizzano le tecnologie digitali al meglio e in modo rispettoso delle regole, di se stessi e degli altri;
- leggono, comprendono ed accettano il documento di eSafety Policy;
- imparano ad essere consapevoli del significato e della gravità di atti di cyberbullismo, a tutela della propria ed altrui incolumità, al fine di evitare violazioni;
- con il supporto della scuola imparano a tutelarsi online, tutelare i/le propri/e compagni/e e rispettarli/le;
- partecipano attivamente a progetti ed attività che riguardano l'uso positivo delle TIC e della Rete e si fanno promotori di quanto appreso anche attraverso possibili percorsi di peer education.

I Genitori

- sono partecipi e attivi nelle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete, nonché sull'uso responsabile dei device personali;
- si relazionano in modo costruttivo con i docenti sulle linee educative che riguardano le TIC e la Rete; inoltre comunicano con loro circa i problemi rilevati quando i/le propri/e figli/e non usano responsabilmente le tecnologie digitali o Internet.

Gli Enti educativi esterni e le associazioni

Gli Enti educativi esterni e le associazioni che entrano in relazione con la scuola devono conformarsi alla politica della stessa riguardo all'uso consapevole della Rete e delle TIC;

Amministratore di sistema

Gestisce la sicurezza, il funzionamento della rete, il controllo degli accessi, la protezione e la conservazione dei dati

---

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).

L'Istituto, all'atto della sottoscrizione del contratto con il personale esterno, qualora si tratti di specialisti che avranno bisogno delle TIC, fornisce informativa riportante le principali regole. Coloro che entreranno a lavorare nell'Istituto dovranno accettare il documento di ePolicy che sarà consultabile sul sito della Scuola.

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.

Per evitare che l'adozione di questa policy rappresenti un mero atto formale, l'Istituto si impegna a prendere spunto da essa come base di partenza per una serie di azioni e iniziative volte a sensibilizzare e informare le singole componenti (personale scolastico, studenti, genitori)

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.

La rilevazione dei casi è compito dell'intera comunità educante qualora ne venisse a conoscenza. E' necessario osservare per tempo ciò che accade per poter agire

immediatamente nei confronti di atti inopportuni, per poter evitare conseguenze più gravi che possono incidere negativamente sul benessere dei minori coinvolti.

Qualora il personale scolastico, non solo la figura docente, dovesse rilevare possibili situazioni di disagio connesse ai rischi correlati ad un uso non responsabile, scorretto o pericoloso delle tecnologie digitali, dovrà informare il Dirigente scolastico.

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

In relazione a quanto specificato in questa policy le infrazioni saranno gestite in modo graduale anche rispetto all'età degli alunni coinvolti.

È bene che i docenti si impegnino a sviluppare nei loro studenti una sempre maggiore consapevolezza dei rischi legati ad un uso imprudente e improprio del web e che forniscano loro, ogni qualvolta avvenga un'infrazione alle regole stabilite, gli strumenti per affrontare le conseguenze dei loro errori.

Nello specifico saranno sanzionate le seguenti infrazioni:

- uso della RETE per giudicare, infastidire, offendere o denigrare qualcuno;
- invio senza permesso di foto o altri dati personali (indirizzo di casa, numero di telefono…..);
- condivisione online di immagini o video di compagni e del personale scolastico senza il loro esplicito consenso o che li ritraggono in pose denigratorie;
- condivisione di immagini intime e/o a sfondo sessuale;
- collegamenti a siti web non adeguati e non indicati dai docenti.

I provvedimenti disciplinari che verranno adottati nei confronti dell'alunno/a che abbia commesso un'infrazione alla policy saranno i seguenti:

- richiamo verbale;
- sanzioni estemporanee commisurate alla gravità della violazione commessa;
- nota informativa sul diario e sul registro alla famiglia;

- convocazione dei genitori.

Il docente Referente per bullismo e cyberbullismo e il Dirigente scolastico saranno il primo punto di contatto per qualsiasi reclamo. Eventuali denunce di bullismo on line saranno trattate in conformità con la normativa vigente, con la possibilità di denunciare l'episodio alla Polizia Postale o garantire, se necessario, un immediato supporto psicologico allo studente attraverso i servizi predisposti.

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.

L'ePolicy, redatta allo scopo di migliorare e rendere più sicuro l'utilizzo delle risorse tecnologiche e di rete, si integra con gli obiettivi e i contenuti del Regolamento d'Istituto e del PTOF. Il Referente del bullismo/cyberbullismo con il gruppo di lavoro, in collaborazione con la Commissione PTOF, in raccordo con il Collegio Docenti, opera al fine di integrare i regolamenti dell'Istituto con il documento ePolicy, apportandone le opportune modifiche da proporre al Consiglio d'Istituto. Tale documento, per una maggiore visibilità e diffusione fra tutti gli attori della comunità educante, sarà presente nel sito web della scuola.

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 monitoraggio dell'implementazione della ePolicy e del suo aggiornamento sarà svolto

orientativamente ogni tre anni partendo da una rilettura dei Piani di azione.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

- **Organizzare 1 evento di presentazione del progetto Generazioni Connesse all'interno della formazione rivolta ai genitori e agli studenti**

Azioni da svolgere nei prossimi 3 anni:

- **Organizzare 1 evento di presentazione del progetto Generazioni Connesse all'interno della formazione rivolta ai genitori e agli studenti secondo le modalità indicate nel capitolo 2**

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.

Il Curricolo delle competenze digitali per gli studenti sarà elaborato nell'a.s. 2021/2022 tenendo presenti le indicazioni del Digicomp, il quadro di riferimento per le competenze dei cittadini.

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.

Nel corso degli anni il nostro Istituto si è organizzato per favorire l'inserimento delle tecnologie informatiche nella didattica (registro elettronico, LIM, aula informatica, aula multimediale, tablet e pc).

Il Collegio Docenti approva la partecipazione del personale docente ad iniziative formative specifiche sulle TIC nella misura di almeno un corso per ogni anno scolastico, al fine di sperimentare le nuove tecnologie nella didattica quotidiana e di coinvolgere anche gli studenti, in relazione all'età, in questo nuovo approccio al sapere e al saper fare.

Le iniziative formative saranno organizzate dall'Istituto facendo ricorso a soggetti esterni e al personale docente interno alla scuola che abbia acquisito competenze sull'innovazione didattica. Saranno altresì divulgate e promosse le proposte formative curate da altri Istituti e dal MIUR. Il percorso della formazione specifica dei docenti sull'utilizzo delle TIC nella didattica deve diventare un processo permanente che deve prevedere anche momenti di autoaggiornamento, di formazione personale o collettiva.

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

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

La formazione degli insegnanti sarà formulata tenuto conto di un'analisi del fabbisogno formativo del corpo docente sull'utilizzo ed integrazione delle TIC nella didattica sulla

base del questionario di autovalutazione relativo al Digcompedu. Al fine di favorire la disseminazione di informazioni circa le opportunità formative interne ed esterne, in presenza e/o a distanza, sarà predisposto sul sito dell'Istituto, una bacheca virtuale dove saranno disponibili contributi e materiali informativi/formativi per le attività di prevenzione, sicurezza, ed un uso consapevole delle TIC, della Rete e dei device fruibili da docenti, studenti e genitori.

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.

L'Istituto, che attraverso la figura dell'Animatore digitale, del Referente per il cyber-bullismo e il gruppo di lavoro ePolicy, ha redatto il presente documento, si impegna alla diffusione delle informazioni e delle procedure per portare a conoscenza delle famiglie i regolamenti sull'utilizzo delle nuove tecnologie e prevenire i rischi legati a un utilizzo non corretto di Internet.

Il Patto di corresponsabilità in particolare richiama il ruolo partecipativo di tutte le componenti della comunità educante coinvolta nella costruzione di percorsi volti a favorire maggiore consapevolezza nell'approccio alle tecnologie informatiche e di contrasto e prevenzione al bullismo e cyberbullismo.

L'Istituto inoltre si propone di continuare a realizzare progetti ed iniziative per coinvolgere e sensibilizzare le famiglie, gli studenti e i docenti su questi temi già a partire dalla scuola dell'infanzia.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2019/2020)

Scegliere almeno 1 di queste azion

- **Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali che verrà ripetuto negli anni a venire.**
- **Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica ricorrendo al DigCompEdu Check-in che verrà ripetuto negli anni a venire.**
- **Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.**
- **Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.**
- **Organizzare incontri con esperti per i genitori in concomitanza di un progetto o percorso che coinvolge anche i ragazzi sui temi dell'educazione all'affettività, alla sessualità e alla cittadinanza digitale. (prevedere 1 tappa per ogni ordine di scuola 3 anni, 7 anni, 11 anni)**
- **Elaborare il curricolo verticale delle competenze digitali degli studenti e delle studentesse**
- **Aggiornamento del Regolamento d'Istituto**
- **Aggiornamento del patto di Corresponsabilità**
- **Creazione all'interno del sito scolastico di spazi divulgativi rivolti a docenti e famiglie**

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

Scegliere almeno 1 di queste azioni

- **Organizzare incontri con esperti per i genitori in concomitanza di un progetto o percorso che coinvolge anche i ragazzi sui temi dell’educazione all’affettività, alla sessualità e alla cittadinanza digitale. (prevedere 2 tappe per ogni ordine di scuola primo e terzo anno scuola infanzia, seconda e quarta classe scuola primaria, prima e terza classe scuola secondaria di primo grado)**

- **Coinvolgere una rappresentanza dei genitori per individuare i temi di maggiore interesse nell’ambito dell’educazione alla cittadinanza digitale.**

- **Organizzare e promuovere per il corpo docente incontri formativi sull’utilizzo e l’integrazione delle TIC nella didattica**

- **Organizzare e promuovere per il corpo docente incontri formativi sull’utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.**

- **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 scolastico in conformità al Regolamento UE 2016/679 si impegna a:

1 redigere e mantenere un registro dei trattamenti dei dati: sia per il titolare che per il responsabile dei trattamenti;

2 valutare i rischi sulla privacy: (definita nel regolamento Data Protection Impact Assessment o PIA) relativamente ad alcune tipologie di trattamento dei dati sensibili, ad esempio, dati relativi alle origini razziali per favorire l'integrazione degli/lle alunni/e, dati relativi alle convinzioni religiose, al fine di garantire la libertà di culto, e dati relativi alla salute per adottare misure di sostegno degli/lle alunni/e.

Il nostro Istituto adotta misure tecniche e organizzative per garantire la sicurezza e la protezione dei dati trattati. Rientrano tra queste:

a) la progettazione del nuovo sito secondo i concetti di privacy by default e by design;

b) l'utilizzo del protocollo HTTPS (l'Hypertext Transfer Protocol Secure è un protocollo per la comunicazione su Internet che protegge l'integrità e la riservatezza dei dati scambiati online);

c) l'utilizzo di un sistema di cifratura quando il trattamento di dati lo richiede;

d) il sistema di backup (sistema che permette di salvare regolarmente i dati; ripristinare eventuali file modificati o rimossi per errore dalla rete; garantire la presenza di una copia di sicurezza di tutti i file importanti);

e) il piano di disaster recovery (insieme di misure che permettono agli apparati di Information technology di superare situazioni di emergenza, ovvero di impedire che imprevisti accidentali o incidenti possano compromettere il funzionamento delle strutture);

f) l'utilizzo di black list per la navigazione (sistemi di filtraggio dei contenuti);

g) l' uso di un firewall hardware (componente hardware che, utilizzando un certo insieme di regole predefinite, permette di filtrare ed eventualmente bloccare tutto il traffico da e verso una qualsiasi rete di computer, lasciando passare solo tutto ciò che

rispetta determinate regole);

h) l'organizzazione di corsi di formazione destinati ai responsabili, agli incaricati ed eventualmente ai subincaricati del trattamento.

In riferimento al d.lgs. 30 giugno 2003, n. 196 (c. d. Codice della Privacy) e al nuovo Regolamento europeo Privacy n. 679/2016, il nostro Istituto predispone un'informativa che illustri la tipologia di dati raccolti, il loro utilizzo e il fine per cui vengono utilizzati; liberatorie specifiche, conformi alla normativa vigente, in materia di protezione dei dati personali.

L'I.C. "Rita Levi-Montalcini" si prefigge di proteggere i dati personali attraverso varie modalità.

Docenti e personale ATA sono responsabili delle password che non possono essere cedute a terze parti e che devono essere mantenute segrete.

Rete Wi-Fi e Personal Computer ad essa collegati: i docenti conoscono le password di accesso alla rete Wi-Fi e quelle per accedere ai singoli pc e sono tenuti alla riservatezza.

E-mail: ogni docente è responsabile del proprio Username e della propria Password di accesso alla casella di posta elettronica istituzionale e si impegna a garantirne la riservatezza e la sicurezza, cambiando almeno una volta all'anno la password di accesso. Tutto il personale è stato avvisato di effettuare sempre e correttamente la procedura di logout da ogni dispositivo utilizzato. Le comunicazioni che avvengono attraverso quest'ultimo canale faranno attenzione a mantenere la riservatezza dell'utenza.

Si ricorda che se si dovesse avere la necessità di conoscere informazioni riservate, si deve far riferimento alla Segreteria: non possono essere scattate fotografie né create/diffuse fotocopie di documenti contenenti dati sensibili. È stato ricordato al personale che le password di accesso al sito, alla rete Wi-Fi e alle mail non dovrebbero essere salvate sui dispositivi dell'Istituto.

L'utenza può comunque consultare l'informativa emendata ai sensi dell'articolo 13 del GDPR per il trattamento dei dati personali al seguente indirizzo: https://www.icmontalcini.edu.it/wp/privacy-policy/

Per il trattamento dei dati personali si fa riferimento al Decreto legislativo 30 giugno 2003, n. 196 e al GDPR Regolamento EU 679/2016. Nello specifico si possono individuare alcune linee guida di e-safety: Si consiglia al personale scolastico di non condividere i propri contatti telefonici e e-mail personali, salvo in occasione di particolari eventi (es. viaggi di istruzione). Si caldeggia, invece, l'utilizzo dei contatti

ufficiali della scuola.

All'atto dell'iscrizione viene richiesto alle famiglie di firmare un'autorizzazione scritta per consentire l'uso di immagini e video delle/dei minori per finalità strettamente connesse alla vita scolastica. Le fotografie o i video da pubblicare sul sito che includano allieve e allievi saranno selezionati tenendo conto dei consensi espressi dai genitori ad inizio anno 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.

Nel regolamento, dunque, una parte sarà dedicata all'uso di Internet in cui gli studenti si impegnano a:

- utilizzare la rete nel modo corretto
- rispettare le consegne dei docenti
- non scaricare materiali e software senza autorizzazione
- non utilizzare unità rimovibili personali senza autorizzazione
- tenere spento lo smartphone al di fuori delle attività didattiche che ne prevedano l'utilizzo
- durante le attività che prevedono lo smartphone, utilizzarlo esclusivamente per svolgere le attività didattiche previste
- segnalare immediatamente materiali inadeguati ai propri insegnanti.

I docenti si impegnano a:

- utilizzare la rete nel modo corretto
- non utilizzare device personali se non per uso didattico
- formare gli studenti all'uso della rete
- dare consegne chiare e definire gli obiettivi delle attività
- monitorare l'uso che gli studenti fanno delle tecnologie a scuola.

Così come previsto dalla legge 71 del 29 maggio 2017, la scuola aggiorna il patto di corresponsabilità con specifici riferimenti a condotte di cyberbullismo.

Informazioni sul regolamento sull'uso delle tecnologie a scuola

Ai fini della migliore accessibilità da parte di genitori del Regolamento sull'uso delle tecnologie a scuola quest'ultimo sarà presentato sul sito dell'Istituto in forma autonoma e non come allegato e sarà diffuso a tutte le componenti scolastiche.

La scuola deve garantire che la navigazione avvenga in sicurezza.

La security sarà implementata attraverso l'adozione delle seguenti misure cautelative:

- Mantenere separate le reti didattica e segreteria: importante per garantire maggiore sicurezza alle informazioni, gestendo in modo autonomo e con regole differenti le due reti grazie al firewall.

- Aggiornare periodicamente software e Sistema operativo: garantire che il sistema sia aggiornato lo protegge dalle aggressioni esterne e dalle vulnerabilità che emergono nel tempo.

-Definire la programmazione di backup periodici: cioè la copia e messa in sicurezza dei dati del sistema scolastico per prevenire la perdita degli stessi (possibilmente anche una copia offline).

-Garantire formazione adeguata allo staff, incluso il corpo docenti: la formazione deve riguardare la gestione dei dispositivi, la conoscenza delle regole basilari sulla sicurezza.

-Preparare piani di azione in risposta ai problemi più seri.

-Definire una policy sulle password.

-Sviluppare il regolamento sull'uso delle tecnologie a scuola (policy di uso accettabile): deve riguardare chiunque abbia accesso alla Rete, studenti/esse, docenti, amministrazione e segreteria, includere i dispositivi della scuola e quelli personali, anche in caso di BYOD.

-Adottare sistemi di filtraggio software e hardware o servizi specifici forniti da Internet provider per bloccare contenuti dannosi o materiali non adatti.

L'IC dispone dell'accesso alla rete wi-fi in tutti i Plessi. La rete è dotata di un firewall per la prevenzione dagli accessi dall'esterno nonché di filtri dei contenuti attraverso l'utilizzo di blacklist e parole chiave in continuo aggiornamento.

L’accesso a Internet è possibile sia nei laboratori informatici, presenti in tutti i plessi dell’Istituto comprensivo, sia nelle aule, dotate di LIM con relativo computer portatile custodito in un cassetto chiuso a chiave. L’accesso a Internet è consentito al personale docente e non docente solo ad esclusivo uso didattico e amministrativo. Gli alunni possono utilizzare, solo per uso didattico, la rete sotto la diretta responsabilità di un insegnante. L’accesso ai dispositivi per la didattica è consentito al personale docente attraverso l’uso di una password.

E-mail: tutti i docenti dell'istituto possiedono una e-mail della scuola del tipo: nome.cognome@icmontalcini.edu.it. Gli alunni, per l’utilizzo delle attività didattiche sono dotati di un indirizzo di posta elettronica della scuola del tipo: nomeutente@icmontalcini.edu.it. Gli indirizzi di posta elettronica sia dei docenti che degli alunni del dominio icmontalcini.edu.it sono gestiti da Google Workspace.

Sito web della scuola: il sito web della scuola è gestito da un team preposto che si adopera affinché il sito sia sicuro e accessibile; ha cura di effettuare aggiornamenti e di intervenire in caso di emergenza. Si usa da alcuni anni il Registro Elettronico.

3.3 - Strumenti di comunicazione online

Le tecnologie digitali sono in grado di ridefinire gli ambienti di apprendimento, supportando la comunicazione a scuola e facilitando un approccio sempre più collaborativo. L’uso degli strumenti di comunicazione online a scuola, al fianco di quelli più tradizionali, ha l’obiettivo di rendere lo scambio comunicativo maggiormente interattivo e orizzontale. Tale uso segue obiettivi e regole precise correlati alle caratteristiche, funzionalità e potenzialità delle tecnologie digitali.

Gli strumenti di comunicazione che vengono utilizzati nel nostro istituto sono:

Il sito web raggiungibile all’indirizzo: https://www.icmontalcini.edu.it.

Il registro elettronico permette una comunicazione chiara ed immediata con le famiglie.

Altra modalità di comunicazione con gli studenti e le famiglie è lo scambio di mail, la pubblicazione di eventi sulla pagina Telegram dell’Istituto e le piattaforme Zoom e Cisco Webex.

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.

Studenti

Come da art.11 del Regolamento d'Istituto non è consentito durante l'intera permanenza dell'alunno all'interno della struttura scolastica (orario scolastico, intervalli, pausa mensa…) sia antimeridiano che pomeridiano, utilizzare dispositivi elettronici personali, quali telefoni cellulari, smartphone, tablet o PC per telefonare, videochiamare, scattare foto, registrare filmati. Tali dispositivi devono essere tenuti rigorosamente spenti e opportunamente custoditi negli zaini. La comunicazione con le famiglie, per qualsiasi urgenza, è sempre garantita attraverso il telefono della scuola. Resta fermo che, anche durante lo svolgimento delle attività didattiche, eventuali esigenze di comunicazione tra gli studenti e le famiglie , dettate da ragioni di particolare urgenza o gravità, potranno sempre essere soddisfatte previa autorizzazione del docente. Qualsiasi uso improprio e non autorizzato prevede il ritiro del dispositivo durante l'orario scolastico e la segnalazione al Dirigente scolastico.

L'utilizzo di strumentazione elettronica personale durante le attività scolastiche, può essere autorizzata esclusivamente per uso didattico e sotto il controllo del docente.

Agli studenti BES, per i quali la scuola garantisce il supporto tecnologico idoneo su richiesta dell'interessato è consentito l'uso della strumentazione personale con l'accesso alla rete wifi dell'Istituto.

Docenti

Durante l'orario di servizio non è consentito l'utilizzo dello smartphone e dispositivi elettronici personali se non per finalità strettamente didattica, così come è consentito

l'uso di altri dispositivi elettronici personali solo a scopo didattico e integrativo di quelli scolastici disponibili. E' consentito l'accesso alla rete wifi della scuola.

Personale della scuola

Durante l'orario di servizio al personale scolastico è consentito l'utilizzo dei dispositivi elettronici personali, quali telefoni cellulari, smartphone, tablet o PC solo per comunicazioni personali di carattere urgente.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2019/2020).

Scegliere almeno 1 di queste azioni:

- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare il personale 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).

Scegliere almeno 1 di queste azioni:

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

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

4.1 - Sensibilizzazione e Prevenzione

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

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

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

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

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

La necessità di sensibilizzare gli studenti ad un utilizzo sicuro e consapevole delle tecnologie digitali, costituisce il primo passo verso un cambiamento positivo. L'Istituto Comprensivo "Rita Levi-Montalcini" persegue azioni di prevenzione e di sensibilizzazione, attraverso un'efficace integrazione con la rete dei servizi territoriali locali (Polizia postale, Associazioni presenti sul territorio, ecc), al fine di formare e

consolidare quelle competenze educative di base necessarie per gestire le situazioni di vita che i ragazzi sperimentano online. Il nostro Istituto attua anche una serie di misure volte a prevenire e contrastare bullismo e cyberbullismo:

-integrazione nel Curricolo di temi legati al corretto utilizzo delle TIC e di Internet; -progettazione di UDA specifiche pianificate a livello di Dipartimenti disciplinari.

Nel nostro Istituto comprensivo, inoltre, è presente un servizio di sportello di ascolto al quale alunni, famiglie e personale possono rivolgersi per avere consigli e sostegno psicologico, anche relativamente alle tematiche del bullismo/cyberbullismo.

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).

Al fine di promuovere sensibilizzazione e prevenzione saranno elaborate proposte diversificate nei diversi ordine di scuola:

-divulgazione di corsi, webinar online ed iniziative aperti ai genitori, riguardo l'educazione al mondo digitale, all'affettività, alla sessualità e allo sviluppo cognitivo, affettivo e relazionale con potenziamento di attività delle life skills secondo i tempi definiti nel cap 2

-divulgazione di corsi ed iniziative aperti agli alunni, riguardo l'educazione al mondo digitale, all'affettività, alla sessualità e allo sviluppo cognitivo, affettivo e relazionale con potenziamento di attività delle life skills secondo i tempi definiti nel cap 2

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.

Inoltre, l'Istituto si potrà avvalere di consulenti/esperti esterni per organizzare incontri formativi rivolti a docenti, genitori ed alunni.

4.4 - Dipendenza da Internet e gioco online

La Dipendenza da Internet fa riferimento all'utilizzo eccessivo e incontrollato di Internet che, al pari di altri comportamenti patologici/dipendenze, può causare o essere associato a isolamento sociale, sintomi da astinenza, problematiche a livello scolastico e irrefrenabile voglia di utilizzo della Rete.

L'istituto è intenzionato a promuovere azioni di prevenzione attraverso percorsi sul benessere digitale?

La Dipendenza da Internet, che può manifestarsi anche attraverso le ore trascorse online a giocare, rappresenta una questione importante per la comunità scolastica. Pertanto il nostro Istituto si prefigge l'obiettivo di fare formazione e di indicare strategie per un uso più consapevole delle tecnologie per favorire il "benessere digitale", cioè la capacità di creare e mantenere una relazione sana con la tecnologia stessa.

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.

Tra le caratteristiche dello stesso vi sono principalmente:

- la fiducia tradita: chi produce e invia contenuti sessualmente espliciti generalmente ripone fiducia nel destinatario;

- la pervasività con cui si diffondono i contenuti: in pochi istanti e attraverso una condivisione che diventa virale, il contenuto può essere diffuso a un numero esponenziale di persone;

- la persistenza del fenomeno: il materiale pubblicato può rimanere online per un tempo illimitato.

Le conseguenze del Sexting hanno ripercussioni negative sulla vittima in termini di autostima, di credibilità e di reputazione sociale.

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.

4.7 - Pedopornografia

La pedopornografia online è un reato (art. 600-ter comma 3 del c.p.) che consiste nel produrre, divulgare, diffondere e pubblicizzare, anche per via telematica, immagini o video ritraenti bambini/e, ragazzi/e coinvolti/e in comportamenti sessualmente espliciti, **concrete o simulate** o qualsiasi rappresentazione degli organi sessuali a fini

soprattutto sessuali.

La legge n. 269 del 3 agosto 1998 *"Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di schiavitù", introduce nuove fattispecie di reato (come ad esempio il turismo sessuale) e, insieme alle successive modifiche e integrazioni contenute nella* ***legge n. 38 del 6 febbraio 2006*** *"Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet"*, segna una tappa fondamentale nella definizione e predisposizione di strumenti utili a contrastare i fenomeni di sfruttamento sessuale a danno di minori. Quest'ultima, introduce, tra le altre cose, il reato di "pornografia minorile virtuale" (artt. 600 ter e 600 quater c.p.) che si verifica quando il materiale pedopornografico rappresenta immagini relative a bambini/e ed adolescenti, realizzate con tecniche di elaborazione grafica non associate, in tutto o in parte, a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali.

Secondo la Legge 172/2012 - *Ratifica della Convenzione di Lanzarote (Art 4.) per pornografia minorile si intende ogni rappresentazione, con qualunque mezzo, di un minore degli anni diciotto coinvolto in attività sessuali esplicite, reali o simulate, o qualunque rappresentazione degli organi sessuali di un minore di anni diciotto per scopi sessuali.*

In un'ottica di attività preventive, il tema della pedopornografia è estremamente delicato, occorre parlarne sempre in considerazione della maturità, della fascia d'età e selezionando il tipo di informazioni che si possono condividere.

La pedopornografia è tuttavia un fenomeno di cui si deve sapere di più, ed è utile parlarne, in particolare se si vogliono chiarire alcuni aspetti legati alle conseguenze impreviste del sexting.

Inoltre, è auspicabile che possa rientrare nei temi di un'attività di sensibilizzazione rivolta ai genitori e al personale scolastico promuovendo i servizi di Generazioni Connesse: qualora navigando in Rete si incontri materiale pedopornografico è opportuno segnalarlo, anche anonimamente, attraverso il sito www.generazioniconnesse.it alla sezione **"Segnala contenuti illegali"** (Hotline).

Il servizio Hotline si occupa di raccogliere e dare corso a segnalazioni, inoltrate anche in forma anonima, relative a contenuti pedopornografici e altri contenuti illegali/dannosi diffusi attraverso la Rete. I due servizi messi a disposizione dal Safer Internet Centre sono il "Clicca e Segnala" di Telefono Azzurro e "STOP-IT" di Save the Children.

In un'ottica di attività preventiva, il tema della pedopornografia è estremamente delicato, occorre parlarne sempre in considerazione della maturità, della fascia d'età e selezionando con cura il tipo di informazioni che si possono condividere.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2019/2020).

Scegliere almeno 1 di queste azioni:

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

□ Organizzare uno o più incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/lle studenti/studentesse.

□ Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/lle studenti/studentesse.

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

Scegliere almeno 1 di queste azioni:

□ Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti agli/lle studenti/studentesse, con il coinvolgimento di esperti.

□ Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti.

□ Organizzare uno o più incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/lle studenti/studentesse.

□ Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/lle studenti/studentesse.

□ Pianificare e realizzare progetti di peer-education - sui temi della sicurezza online - nella scuola.

Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

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

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

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

Nelle procedure:

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

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

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

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

Questo risulta importante sia per facilitare l'emersione di situazioni a rischio, e la conseguente presa in carico e gestione, sia per dare un messaggio chiaro a studenti e

studentesse, alle famiglie e a tutti coloro che vivono la scuola che la stessa è un luogo sicuro, attento al benessere di chi lo vive, in cui le problematiche non vengono ignorate ma gestite con una mobilitazione attenta di tutta la comunità.

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

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

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

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

Vi suggeriamo, inoltre, i seguenti servizi:

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

- Clicca e segnala di Telefono Azzurro e STOP-IT di Save the Children Italia per

segnalare la presenza di materiale pedopornografico online.

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.

Per quanto riguarda la gestione dei casi, il nostro Istituto ha individuato una figura Referente per il cyberbullismo. La segnalazione del caso dovrà quindi essere fatta dal singolo docente alla Referente, la quale si occuperà di raccogliere tutte le informazioni possibili, anche attraverso colloqui di approfondimento con gli attori coinvolti e di segnalare l'accaduto al Dirigente scolastico. Sarà poi il Dirigente ad informare famiglie degli alunni coinvolti e a valutare se informare organi esterni o se il caso vada gestito all'interno della scuola, con il coinvolgimento del Consiglio di Classe. Si sceglierà uno o più interventi da attuare a cui seguirà una fase di monitoraggio.

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.

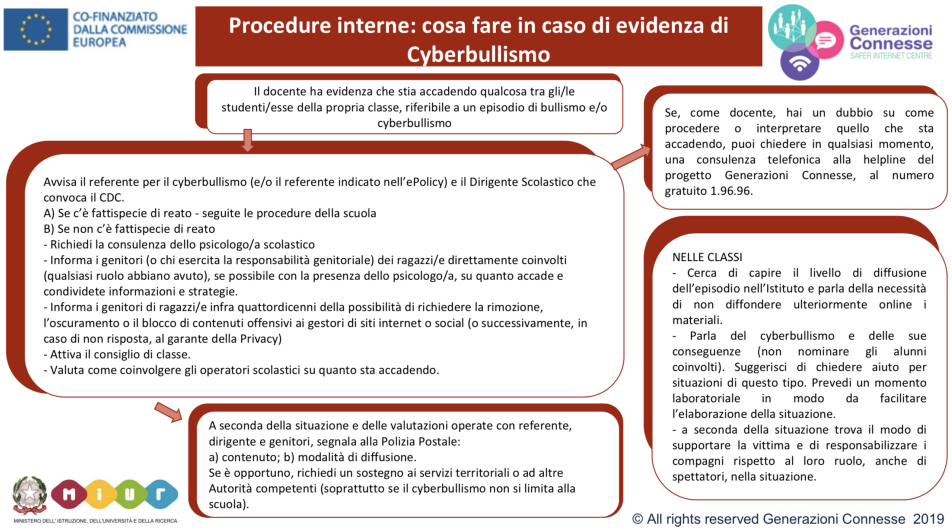
- **Comitato Regionale Unicef**: laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni)**: svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare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

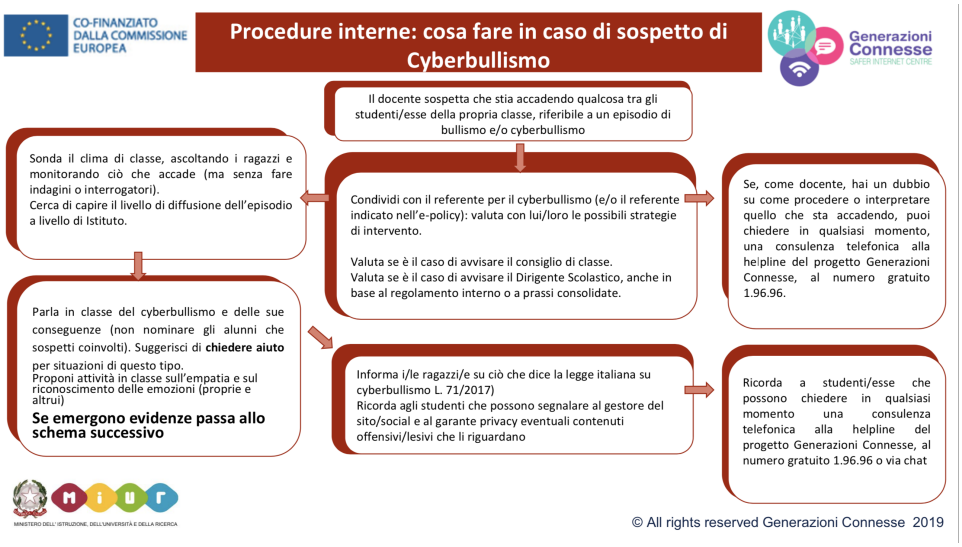
psicologico o psichiatrico delle situazioni problematiche vissute in Rete. In alcune regioni, come il Lazio e la Lombardia, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da Internet e alle situazioni di rischio correlate.

- **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.

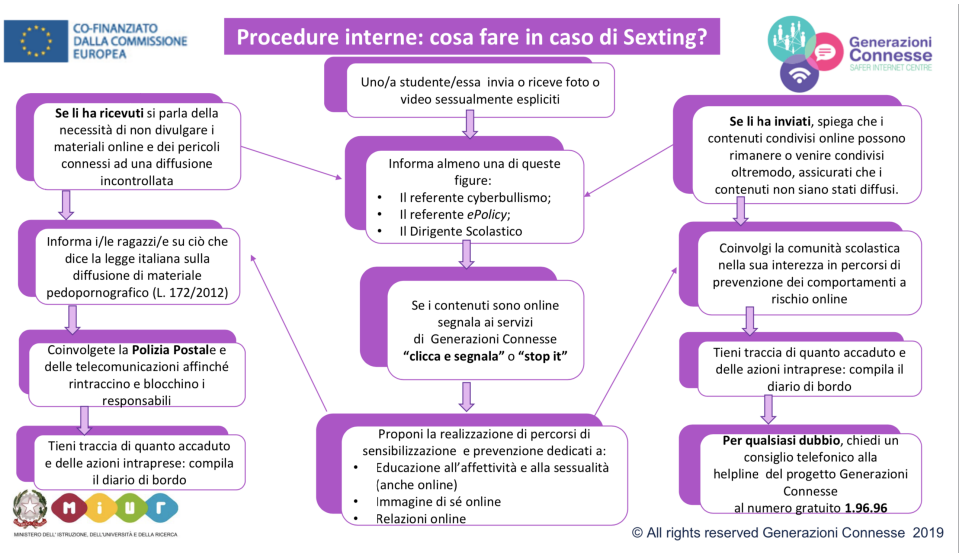
5.4. - Allegati con le procedure

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

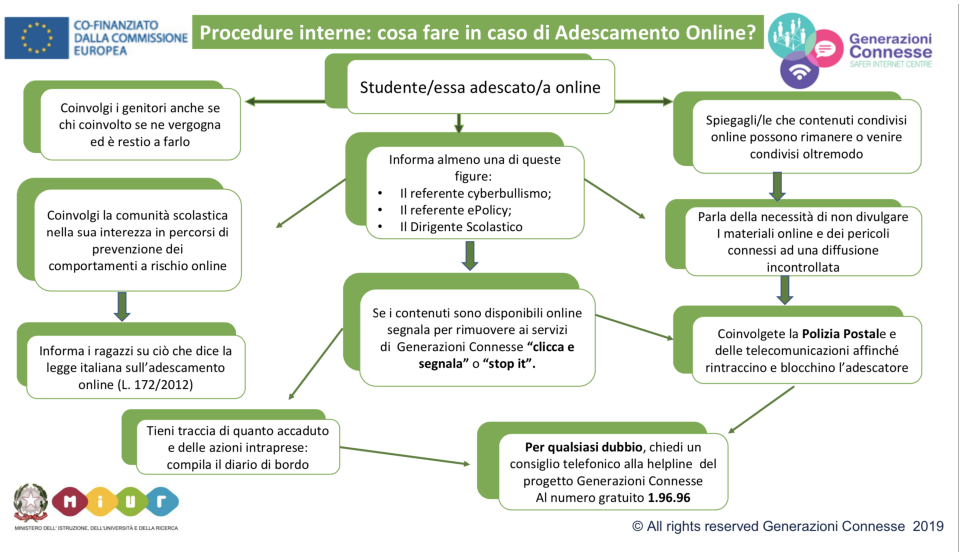




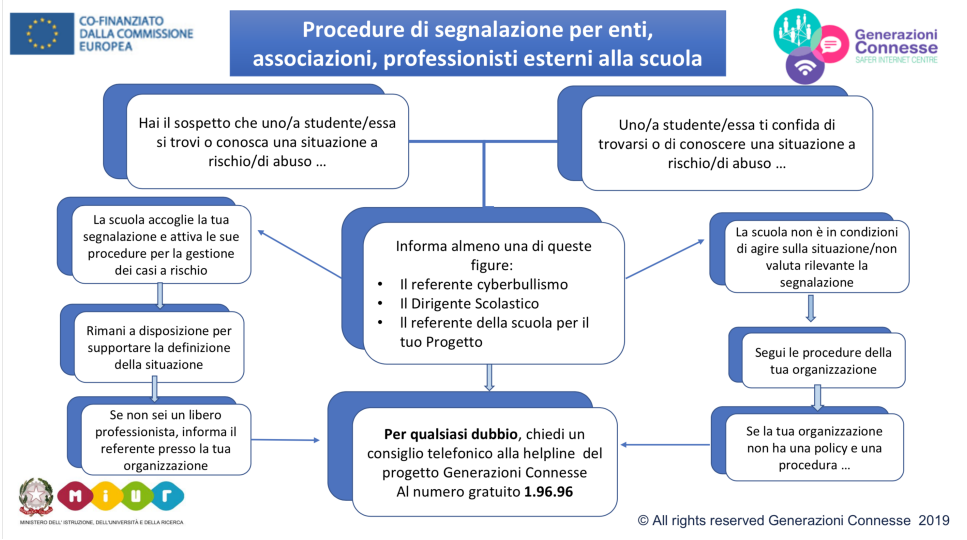
Procedure interne: cosa fare in caso di sexting?



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

Per la gestione dei casi si individuano 3 livelli a seconda della gravità e del grado di rischio.

- Primo livello, per i casi in cui si registri un comportamento moderatamente rischioso o scorretto ma non classificabile come bullismo (ad esempio interazioni aggressive e poco rispettose nelle chat), i docenti intervengono attraverso la normale attività educativa, di richiamo al rispetto delle regole di convivenza civile e democratica, di rispetto degli altri, per evitare che possano degenerare, diventare pericolosi per sé o offensivi e minacciosi per gli altri.

- Secondo livello, casi di bullismo o cyberbullismo: accertato il caso di bullismo o cyberbullismo, informati il Referente e il Dirigente, i docenti provvedono a realizzare interventi mirati sul gruppo classe, eventualmente anche in collaborazione con associazioni e altre agenzie educative presenti sul territorio, comprese le forze dell'ordine. Esempi di intervento possono essere gruppi di discussione (circle time), con rappresentazioni e attività di role-play sull'argomento del bullismo, attività di problem solving. Se necessario, verranno intrapresi anche percorsi individualizzati nei confronti della vittima e del bullo/i. Inoltre la scuola, qualora rilevi una situazione psico-socio-educativa particolarmente problematica, convocherà i genitori o gli esercenti la potestà per valutare con loro a quali risorse territoriali possono rivolgersi.

- Terzo livello, casi in cui si registrano gravi infrazioni: per tutelare la vittima, nei casi più gravi, si ricorre all'Autorità Giudiziaria e agli organi di Polizia.

In caso di necessità si terranno presenti i seguenti riferimenti a livello nazionale:

- Telefono azzurro (chat anonima o numero verde 19696)

- Save the Children

- Numero verde 800669696 (Ministero della Pubblica Istruzione: campagna "Smonta il bullo")

Numero verde 114 per segnalare situazioni emergenziali di disagio riguardanti l'infanzia e l'adolescenza