Documento di ePolicy

BGVC010005

C. BATTISTI

VIA CESARE BATTISTI 1 - 24065 - LOVERE - BERGAMO (BG)

Federico Spandre

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.

In particolare, in base alle Linee Guida per l'Uso delle Tecnologie Digitali e la Prevenzione dei Rischi delle scuole (MIUR, 2019), la scuola si impegna a:

- adottare una strategia integrata e globale che coinvolge tutti gli attori della scuola, studenti e studentesse, docenti, educatori, genitori, e personale ATA;
- adottare una politica di prevenzione;
- segnalare e prendere in carico situazioni potenzialmente a rischio;
- valutare i bisogni e definire gli obiettivi per sensibilizzare sui rischi legati all'uso delle tecnologie digitali e per affrontare situazioni di rischio già verificatesi;
- promuovere l'educazione al rispetto, lo sviluppo del pensiero critico e la promozione dell'Educazione Civica Digitale;
- valutare gli interventi al fine di promuovere pratiche di comprovata efficacia;
- proteggere i dati personali.

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.

Il **Dirigente Scolastico** garantisce la sicurezza, anche online, di tutti i membri della comunità scolastica. Promuove la cultura della sicurezza online e, ove possibile, dà il proprio contributo all'organizzazione, insieme al docente referente sulle tematiche del bullismo/cyberbullismo, di corsi di formazione specifici per tutte le figure scolastiche sull'utilizzo positivo e responsabile delle TIC. Inoltre, ha la responsabilità di gestire e intervenire nei casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali.

L'**animatore digitale** supporta il personale scolastico da un punto di vista non solo tecnico-informatico, ma anche in riferimento ai rischi online, alla protezione e gestione dei dati personali, ed è uno dei promotori di percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale". Monitora e rileva eventuali episodi o problematiche connesse all'uso delle TIC a scuola, e ha il compito di controllare che gli utenti autorizzati accedano alla Rete della scuola con apposita password, per scopi istituzionali e consentiti (istruzione e formazione).

Il **referente per il bullismo e cyberbullismo** (nominato secondo l'Art. 4 Legge n.71/2017) ha il compito di coordinare e promuovere iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo. A tal fine, può avvalersi della collaborazione delle Forze di polizia, delle associazioni e dei centri di aggregazione giovanile del territorio.

I **docenti** e gli **educatori** hanno un ruolo centrale nel diffondere la cultura dell'uso responsabile delle TIC e della Rete. Devono accompagnare e supportare gli studenti e le studentesse nelle attività di apprendimento e nei laboratori che prevedono l'uso della LIM o di altri dispositivi tecnologici che si connettono alla Rete. Hanno il dovere morale e professionale di segnalare al Dirigente Scolastico qualunque problematica, violazione o abuso, anche online, che vede coinvolti studenti e studentesse.

Il **personale Amministrativo, Tecnico e Ausiliario (ATA)** deve segnalare comportamenti non adeguati e/o episodi di bullismo/cyberbullismo, insieme ad altre figure e raccoglie, verifica e valuta le informazioni inerenti a possibili casi di bullismo/cyberbullismo.

Gli **studenti e le studentesse** devono, in relazione al proprio grado di maturità e consapevolezza raggiunta, utilizzare al meglio le tecnologie digitali in coerenza con quanto richiesto dai docenti. Con il supporto della scuola devono imparare a tutelarsi online, tutelare i/le propri/e compagni/e e rispettarli/le e partecipano attivamente a progetti ed attività che riguardano l'uso positivo delle TIC e della Rete, facendosi promotori di quanto appreso anche attraverso possibili percorsi di *peer education*.

I **genitori**, in continuità con l'Istituto scolastico, devono essere partecipi e attivi nelle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete, nonché sull'uso responsabile dei device personali. Devono relazionarsi in modo costruttivo con i docenti sulle linee educative che riguardano le TIC e la Rete e comunicare 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** che entrano in relazione con la scuola devono conformarsi alla politica della stessa riguardo all'uso consapevole della Rete e delle TIC e promuovere comportamenti sicuri, la sicurezza online e assicurare la protezione degli studenti e delle studentesse durante le attività che si svolgono insieme.

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).

Gli Enti educativi esterni e le associazioni che entrano in relazione con la scuola vengono informati riguardo alle regole di comportamento che devono essere seguite dagli studenti e dalle studentesse e da tutte le figure educanti. In particolare, si fornirà un'informativa sintetica sull'ePolicy comprensiva delle procedure di segnalazione in modo che siano tutelati gli studenti, le studentesse e la scuola stessa e per porre in essere nuove modalità per rilevare, limitare e contrastare possibili pericoli legati a condotte educative non professionali.

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.

Condividere e comunicare il documento agli studenti e alle studentesse significa dare loro una base di partenza per un uso consapevole e maturo dei dispositivi e della tecnologia informatica. In questo modo, hanno a disposizione regole condivise di sicurezza circa il comportamento da tenere a scuola e nei contesti extrascolastici ed elementi per poter riconoscere e quindi prevenire comportamenti a rischio sia personali che dei/delle propri/e compagni/e.
È importante condividere e comunicare il documento al personale scolastico in modo da poter orientare tutte le figure sui temi in oggetto, a partire da un uso corretto dei dispositivi e della Rete in linea anche con il codice di comportamento dei pubblici dipendenti.
È fondamentale condividere e comunicare il documento ai genitori sul sito istituzionale della scuola, nonché tramite momenti di formazione specifici e durante gli incontri scuola-famiglia.

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.

Si seguiranno le indicazioni integrate nel Regolamento d'Istituto e nel Patto di Corresponsabilità.
Per esempio, si tratteranno casi che riguardano:

- la condivisione online di immagini o video di compagni/e senza il loro consenso o che li ritraggono in pose offensive e denigratorie;
- la condivisione di scatti intimi e a sfondo sessuale;
- la condivisione di dati personali;
- l'invio di immagini o video volti all'esclusione di compagni/e.

1.6 - Integrazione dell'ePolicy con Regolamenti esistenti

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

1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

L'E-policy viene aggiornata periodicamente e quando si verificano cambiamenti significativi in riferimento all'uso delle tecnologie digitali all'interno della scuola. Le modifiche del documento saranno discusse con tutti i membri del personale docente. Il monitoraggio del documento sarà realizzato a partire da una valutazione della sua efficacia in riferimento agli obiettivi specifici che lo stesso si pone.

da compilare con le indicazioni contenute nella lezione

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

- **2019/2020** Creazione del gruppo di lavoro ePolicy
- **2020/2021** Realizzazione di un sistema di monitoraggio delle attività *(Azione sviluppabile nell'arco di un anno)*
- **2020/2021** Realizzazione di un'assemblea per discutere delle attività di progetto *(Azione sviluppabile nell'arco di un anno)*

Azioni da svolgere nei prossimi 3 anni:

- Monitoraggio delle attività e aggiornamento dell'ePolicy, del Regolamento d'Istituto e del Patto di Corresponsabilità *(Azione sviluppabile nell'arco di due anni)*

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 lavoro in classe, seguendo le "Raccomandazioni Europee", deve essere integrato da competenze che richiamino le dimensioni tecnologiche, cognitive, etiche e sociali.

- **Dimensione tecnologica**: è importante far riflettere i più giovani sul potenziale delle tecnologie digitali come strumenti per la risoluzione di problemi della vita quotidiana, onde evitare automatismi che abbiano conseguenze incerte, attraverso un'adeguata comprensione della "grammatica" dello strumento.
- **Dimensione cognitiva**: fa riferimento alla capacità di cercare, usare e creare in modo critico le informazioni condivise in Rete, valutandone credibilità e affidabilità.
- **Dimensione etica e sociale**: la prima fa riferimento alla capacità di gestire in modo sicuro i propri dati personali e quelli altrui, e di usare le tecnologie digitali per scopi eticamente accettabili e nel rispetto degli altri. La seconda, invece, pone un po' più l'accento sulle pratiche sociali e quindi sullo sviluppo di particolari abilità socio-comunicative e partecipative per maturare una maggiore consapevolezza sui nostri doveri nei riguardi di coloro con cui comunichiamo online.

A tal proposito:

- alcune classi della scuola primaria seguono corsi di coding;
- le classi della scuola secondaria di primo grado sono coinvolte nel progetto “sicurezza e prevenzione” e “computer grafica”;
- alcune classi del liceo partecipano alle campagne promosse dal ministero e dalle associazioni sul territorio relative al tema del bullismo/cyberbullismo.

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.

I docenti dell’istituto, di ogni ordine e grado, e gli educatori integrano le conoscenze già acquisite, con corsi individuali e liberamente scelti.

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.

Al fine di approfondire il fabbisogno dell'Istituto occorre:

- ascoltare le richieste degli insegnanti, degli educatori e degli studenti sull'uso sicuro della Rete;
- promuovere la partecipazione dei docenti e degli educatori a corsi di formazione, in presenza e online, che abbiano ad oggetto i temi del progetto "Generazioni Connesse";
- organizzare incontri con professionisti della scuola o con esperti esterni, enti/associazioni, etc.

2.4. - Sensibilizzazione delle famiglie e integrazioni al Patto di Corresponsabilità

Nella prevenzione dei rischi connessi ad un uso non consapevole delle TIC, così come nella promozione di un loro uso positivo e capace di coglierne le opportunità, è necessaria la collaborazione di tutti gli attori educanti, ognuno secondo i propri ruoli e le proprie responsabilità. Scuola e famiglia devono rinforzare l'alleanza educativa e promuovere percorsi educativi continuativi e condivisi per accompagnare insieme ragazzi/e e bambini/e verso un uso responsabile e arricchente delle tecnologie digitali, anche in una prospettiva lavorativa futura. L'Istituto garantisce la massima informazione alle famiglie di tutte le attività e iniziative intraprese sul tema delle tecnologie digitali, previste dall'ePolicy e dal suo piano di azioni, anche attraverso l'aggiornamento, oltre che del regolamento scolastico, anche del "Patto di corresponsabilità" e attraverso una sezione dedicata sul sito web dell'Istituto.

La scuola offre opportunità di incontro e ascolto, per richieste in continua evoluzione, ciò in continuità anche con l'art. 5 (comma 2) della legge 29 maggio 2017, n.71 "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo" che prevede l'integrazione, oltre che del regolamento scolastico, anche del "Patto di Corresponsabilità", con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari "commisurate alla gravità degli atti compiuti", al fine di meglio regolamentare l'insieme dei provvedimenti sia di natura disciplinare che di natura educativa e di prevenzione al fenomeno.

Il nostro piano d'azioni

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

Si propone il corso di Generazioni Connesse che contiene anche queste tematiche:

- organizzare e promuovere per il corpo docente e per gli educatori incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.

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

2020/2021

Con Google Moduli questionario per analizzare le seguenti tematiche (insieme a quelle del Capitolo 3):

- fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali;
- fabbisogno formativo del corpo docente e degli educatori sull'utilizzo e l'integrazione delle TIC nella didattica;
- fabbisogno formativo del corpo docente e degli educatori sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali;
- coinvolgere una rappresentanza dei genitori per individuare i temi di maggiore interesse nell'ambito dell'educazione alla cittadinanza digitale.

2020/2021 - 2021/2022

- Organizzare e promuovere per il corpo docente e per gli educatori incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare incontri con esperti per i docenti e per gli educatori sulle competenze digitali.
- Organizzare e promuovere per il corpo docente e per gli educatori incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare incontri con esperti per i genitori sull'educazione alla cittadinanza digitale.

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.

In fase di iscrizione degli alunni alla scuola i genitori sottoscrivono un'informativa sul trattamento dei dati personali in ottemperanza con gli artt.13-14 GDPR 2016/679 e d.lgs.101/2018.
All'inizio dell'anno scolastico i genitori rilasciano il consenso all'utilizzo di materiale fotografico e audiovisivo riservato ed elaborati degli alunni per esporli anche in sedi diverse da quelle dell'Istituto quali pubblicazioni in formato digitale e siti WEB.
In caso di utilizzo di piattaforme digitali condivise o di strumenti per la creazione e la gestione di classi virtuali viene acquisito preventivamente il consenso informato dei genitori. In caso di attività di ampliamento dell'offerta formativa, organizzate in collaborazione con Enti esterni, viene richiesto preventivamente ai genitori il consenso informato alle riprese audio/ video e al loro eventuale utilizzo per scopi didattici, informativi e divulgativi anche tramite pubblicazione sul sito web del Convitto. In un'ottica di massima trasparenza nei confronti dei soggetti interessati, il Gruppo Spaggiari Parma S.p.A. (azienda che gestisce il registro elettronico e il sito wb dell'Istituto) precisa che, in ragione degli specifici accordi contrattuali intercorrenti tra Gruppo Spaggiari Parma S.p.A. e **Convitto Nazionale Cesare Battisti Lovere**, questi ultimi sono i titolari del trattamento dei dati personali dell'utente-soggetto interessato all'interno della piattaforma internet denominata "**PrimaVisioneWeb**" (di seguito l'"**Applicazione**"), mentre Gruppo Spaggiari Parma S.p.A. opera quale Responsabile del trattamento designato ai sensi dell'art. 28 del GDPR dal titolare del trattamento. Pertanto, per ogni ulteriore informazione in merito al trattamento dei propri dati personali condotto all'interno dell'Applicazione, ivi incluso il rilascio dell'informativa per il trattamento dei dati personali ex art. 13 del GDPR, l'utente-soggetto interessato dovrà rivolgersi al titolare del trattamento, da intendersi quale il proprio istituto scolastico di riferimento. Gruppo Spaggiari Parma S.p.A. resta, in ogni caso, a disposizione dell'utente-soggetto interessato per ogni eventuale ulteriore chiarimento in merito a quanto sopra, al seguente indirizzo e-mail privacy@spaggiari.eu.

3.2 - Accesso ad Internet

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

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

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

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

Il parco macchine online del Convitto Nazionale Cesare battisti può essere suddiviso nel seguente modo:

Scuola primaria

- Laboratorio di informatica con 24 unità notebook con Windows 7 professional che risultano collegate con rete wifi dell'Istituto. L'accesso degli studenti è regolamentato da un account specifico con restrizioni per quanto riguarda sia la navigazione sia la possibilità di effettuare download. L'intero laboratorio è sottoposto a firewall.

Scuola secondaria di primo grado

- Laboratorio di informatica con 30 + 4 unità fisse (macchine virtuali) che risultano collegate con rete interna alla sala server dell'Istituto. L'accesso degli studenti è regolamentato da un account specifico con restrizioni per quanto riguarda sia la navigazione sia la possibilità di effettuare download. L'intero laboratorio è sottoposto a firewall.
- Laboratorio mobile costituito da 28 tablet che accedono ad internet via wifi. Le macchine sono dotate di account univoco e vengono utilizzate dagli studenti solo durante le attività didattiche e sotto la supervisione diretta dell'insegnante. L'accesso degli studenti è regolamentato da un account specifico con restrizioni per quanto riguarda sia la navigazione sia la possibilità di effettuare download. L'intero laboratorio è sottoposto a firewall.
- Nelle 9 classi più aula di arte ed immagine della scuola sono presenti notebook con Windows 10 collegati alla rete tramite rete lan. Le macchine sono dotate di account univoco e vengono utilizzate dagli studenti solo durante le attività didattiche e sotto la supervisione diretta dell'insegnante. L'accesso degli studenti è regolamentato da un account specifico con restrizioni per quanto riguarda sia la navigazione sia la possibilità di effettuare download.

L'intero laboratorio è sottoposto a firewall.

Scuola secondaria di secondo grado: Liceo linguistico

- Laboratorio mobile costituito da 30 notebook con Windows 10 che accedono ad internet via wifi. Le macchine sono dotate di account univoco e vengono utilizzate dagli studenti solo durante le attività didattiche e sotto la supervisione diretta dell'insegnante. L'accesso degli studenti è regolamentato da un account specifico con restrizioni per quanto riguarda sia la navigazione sia la possibilità di effettuare download. L'intero laboratorio è sottoposto a firewall.
- Laboratorio mobile costituito da 25 notebook con Windows 10 che accedono ad internet via wifi. Le macchine sono dotate di account univoco e vengono utilizzate dagli studenti solo durante le attività didattiche e sotto la supervisione diretta dell'insegnante. L'accesso degli studenti è regolamentato da un account specifico con restrizioni per quanto riguarda sia la navigazione sia la possibilità di effettuare download. L'intero laboratorio è sottoposto a firewall.
- Nelle 10 classi del liceo sono presenti notebook con Windows 10 collegati alla rete tramite rete lan. Le macchine sono dotate di account univoco e vengono utilizzate dagli studenti solo durante le attività didattiche e sotto la supervisione diretta dell'insegnante. L'accesso degli studenti è regolamentato da un account specifico con restrizioni per quanto riguarda sia la navigazione sia la possibilità di effettuare download.

Dotazione tecnica rete e filtri

- L'istituo è dotato di 2 linee fibra da 100 Mbps in download e 20 Mbps in Upload. La prima serve esclusivamente il liceo linguistico, la senda linea è condivisa tra la scuola primaria e la secondaria di primo grado.
- La segreteria dell'istituto è dotata di server autonomi e di una linea adsl business dedicata.
- L'intero istituto è dotato di un firewall MikroTik da cui vengono generate le Vlan dell'istituto che sono gestite sia a livello Lan e Wifi da autenticazione Hotspot.
- I docenti ed il personale educativo dell'istituto può connettersi alla Wifi con dispositivi personali previo login di autenticazione univoco e nominale. Tutto il traffico della rete viene monitorato dal software Wi4school e dal filtro dei contenuti nPxCloud.

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.

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

3.4 - Strumentazione personale

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

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

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

Il sito istituzionale della scuola https:www.convittolovere.edu.it è attivo e gestito da un responsabile amministratore nominato dal dirigente.

L'amministratore del sito è coadiuvato da un team che contribuisce alla fornitura e alla pubblicazione dei contenuti online.

Il nostro piano d'azioni

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

2020/2021

Con Google Moduli questionario anche con le tematiche del capitolo 2:

- Effettuare un’analisi sull’utilizzo dei dispositivi personali a scuola da parte degli studenti e delle studentesse.
- Effettuare un’analisi sull’utilizzo dei dispositivi personali a scuola da parte dei

docenti e degli educatori.

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte del personale Tecnico Amministrativo e dagli ATA.

- Organizzare uno o più eventi o attività volti a consultare i docenti e gli educatori dell'Istituto per redigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali.

2021/2022

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

- Organizzare uno o più eventi o attività volti a formare 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 i genitori dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali.

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

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

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.*

L'Istituto propone una serie di approfondimenti relativi al tema attraverso la partecipazione a spettacoli teatrali e campagne promosse dal MIUR e a conferenze e interventi di personalità esperte nel settore; inoltre, sono previsti visioni di film e letture a tema in orario curricolare. Nel corrente anno scolastico per l'istituto comprensivo si propone un progetto sulla legalità, nella quale rientrano approfondimenti sul tema del bullismo e del cyberbullismo. La scuola, inoltre, propone annualmente l'acquisto di libri di testo per sensibilizzare al tema.

La sensibilizzazione può costituire il primo passo verso un cambiamento positivo ma, per far sì che l'intervento sia efficace, è importante che sia chiara l'azione verso cui i soggetti devono impegnarsi.

La prevenzione parte dal presupposto che tutti gli studenti siano potenzialmente a rischio. Si tratta quindi di interventi diretti al grande pubblico o a un intero gruppo di una popolazione che non è stato identificato sulla base del rischio individuale. Questi interventi possono produrre cambiamenti all'interno della comunità scolastica perché vanno a formare e consolidare quelle competenze educative di base necessarie a poter gestire le situazioni di vita che i/le ragazzi/e sperimentano online. Solo attraverso la conoscenza del problema possono essere attuate tutte le misure necessarie alla sua prevenzione.

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).

Le caratteristiche specifiche del cyberbullismo rispetto al bullismo cosiddetto tradizionale, secondo i più recenti studi, possono essere ricondotte ai seguenti tratti specifici.

- **L'impatto**: la diffusione di materiale tramite Internet è incontrollabile e non è possibile prevederne i limiti (anche se la situazione migliora, video e immagini potrebbero restare online e continuare a diffondersi). Un contenuto offensivo e denigratorio online può, quindi, diventare virale e distruggere in alcuni casi la reputazione della vittima.
- **La convinzione dell'anonimato**: chi offende online potrebbe tentare di rimanere nascosto dietro un nickname e cercare di non essere identificabile. Sentendosi protetti dall'anonimato ci si sente liberi e più forti nel compiere atti denigratori, senza il timore di essere scoperti.
- **L'assenza di confini spaziali**: il cyberbullismo può avvenire ovunque, invadendo anche gli spazi personali e privando l'individuo dei suoi spazi-rifugio.
- **L'assenza di limiti temporali**: può avvenire a ogni ora del giorno e della notte.
- **L'indebolimento dell'empatia**: esistono cellule chiamate neuroni specchio che ci permettono di "leggere" gli altri quando li abbiamo di fronte, capirli e di provare emozioni simile a quelle che loro provano, proprio come se fossimo di fronte ad uno specchio. Tale sensazione è data dall'attivazione di una particolare area del cervello. Quando le interazioni avvengono prevalentemente online la funzione speciale di questi neuroni viene meno (mancando la presenza fondamentale dell'altro che è sostituito dal dispositivo). La riduzione di empatia che ne consegue può degenerare nei comportamenti noti messi in atto dai cyberbulli.
- **Il feedback non tangibile**: il cyberbullo non vede in modo diretto le reazioni della vittima e, ancora na volta, ciò riduce fortemente l'empatia e il riconoscimento del danno provocato.

A ciò si deve inoltre aggiungere alcune semplici considerazione. La prima, la percezione che online non ci siano norme sociali da rispettare: fra i giovani spesso vige la falsa convinzione secondo cui la Rete sia uno spazio virtuale lontano dalla realtà, in cui vige libertà assoluta e in cui regole e norme sociali della vita quotidiana non valgono. La seconda, la sperimentazione online di identità e personalità multiple: la Rete è per i minori il luogo virtuale per eccellenza in cui mettersi in gioco "fingendo di essere ciò che non si è" per il semplice gusto di sperimentare nuove forme di identità e comportamento. Inoltre, non meno importante la diffusione di responsabilità; tutti quelli che partecipano anche solo con un like o un commento diventano, di fatto, corresponsabili delle azioni del cyberbullo facendo accrescere la portata dell'azione; mettere un "like" su un social network commentare o condividere una foto o un video che prende di mira qualcuno o semplicemente tacere pur sapendo, mette ragazzi e ragazze nella condizione di avere una responsabilità.

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.

Il nostro istituto si impegna a promuovere attività di analisi e produzione mediale, finalizzate soprattutto a:

- 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.

In particolare, verrà approfondito nelle classi il documento *No Hate Speech* del Consiglio d'Europa, nella versione in italiano.

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?

Secondo uno studio del King's College di Londra più del 23% dei giovani intervistati ha una relazione disfunzionale con il proprio smartphone. Stati d'ansia provocati dalla ricerca e dall'uso compulsivo del cellulare che, nei casi più gravi, si associano a veri e propri stati depressivi. In Italia, secondo una ricerca, ben il 45% degli studenti (6.671 giovani tra gli 11 e i 25 anni) dichiara di passare sul web almeno 5-6 ore ogni giorno e il tempo trascorso online raggiunge picchi più alti nel fine settimana: 1 intervistato su 5 dice di sentirsi a disagio o comunque va in ansia quando manca la connessione alla Rete e cresce in contemporanea la percentuale di coloro che manifestano attacchi di panico quando finiscono i giga e le promozioni tariffarie a cui sono abbonati (circa 1 su 3).

Di seguito i sintomi che devono essere presenti (per un arco di tempo di almeno un anno):

- il giocatore è assorbito totalmente dal gioco;
- il giocatore è preoccupato e ossessionato dal gioco (si veda Lancini M., Il ritiro sociale negli adolescenti, Raffaello Cortina Ed., Milano, 2019);
- il gioco consente alla persona di sfuggire alla realtà con la sperimentazione di emozioni più piacevoli;
- il giocatore manifesta sempre di più l'impulso di giocare e di sperimentare emozioni positive;
- il giocatore sente di dover dedicare più tempo ai giochi;
- il giocatore se non può giocare manifesta ansia, depressione e irritabilità;
- può emergere un ritiro sociale (si veda il punto 3);
- il giocatore, anche se comprende la gravità della situazione e sospende di giocare comunque non riesce a interrompere del tutto;
- il giocatore mente agli altri sull'utilizzo che fa dei giochi on line;
- il giocatore ha perso o mette a rischio relazioni o opportunità a causa dei giochi su Internet.

Ad oggi nella nostra scuola non si sono verificati casi di questa tipologia, tuttavia nelgli anni a venire anche in collaboazione con la psicologa della scuola, gli enti comprensoriali e le associazioni del settore si svolgeranno delle inziative volte a favorire la cooscneza della dipendenza da gioco. Un primo momento formativo può essere costitutito dalla riflessione in classe sul tempo trascorso online, sul valore aggiunto o meno che questo tempo produce nelle noestre vite, sul ruolo che deve avere la tecnologia nelle nsotre vite.

Allo stesso modo quando parliamo di videogiochi, dobbiamo pensarli non in termini negativi ma di benessere digitale. Sono parte del mondo di studenti e studentesse. E, allora, riflettiamo insieme a ragazzi e ragazze su: quando sono una risorsa? Accedono a contenuti adeguati all'età? A che ora e per quanto tempo li usano? Diventa utile riflettere con i ragazzi e le ragazze rispetto all'uso della tecnologia in termini di qualità e tempo.

Se controlliamo la tecnologia possiamo usarne il pieno potenziale e trarne vantaggi.

Strutturare regole condivise e stipulare con loro una sorta di "patto" d'aula e, infine, proporre delle alternative metodologiche e didattiche valide che abbiano come strumento giochi virtuali d'aula (per esempio adoperando la LIM o il dispositivo personale). È importante, quindi, non demonizzare la tecnologia o il gioco, ma cercare di entrare nel mondo degli/lle studenti e delle studentesse, stabilendo chiare e semplici regole di utilizzo.

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.

Secondo una recente ricerca di Scuola.net per la Polizia di Stato - ricerca che ha coinvolto 6.500 ragazzi tra i 13 e i 18 anni - il 24% di loro ha scambiato almeno una volta immagini intime con il partner via chat o social (fenomeno conosciuto come sexting). Tra questi, il 15% ha subito la condivisione con terzi, senza consenso, di questo materiale. Il motivo più frequente, riportato dalle vittime? Un banale “scherzo” (49%), a dimostrazione di quanto possano essere sottovalutate le reali conseguenze di tale diffusione. Tra le altre motivazioni, il ricatto (11%) o la vendetta (7%): il revenge porn, pure presente, viene surclassato dalla leggerezza e dalla goliardia ma gli effetti sono drammaticamente gli stessi. La reazione più diffusa nella maggior parte dei casi è il silenzio: il 53% ha fatto finta di niente, il 31% non ha detto nulla per non essere giudicato.

Il sexting (abbreviazione di sex – sesso e texting – messaggiare, inviare messaggi) indica l’invio e/o la ricezione di contenuti (video o immagini) sessualmente espliciti che ritraggono se stessi o gli altri.

I rischi del sexting, legati al revenge porn, possono contemplare: violenza psicosessuale, umiliazione, bullismo, cyberbullismo, molestie, stress emotivo che si riversa anche sul corpo insieme ad ansia diffusa, sfiducia nell’altro/i e depressione.

Ad oggi nella nostra scuola non si sono verificati casi di questa tipologia, tuttavia nelgli anni a venire anche in collaboazione con la psicologa della scuola, gli enti comprensoriali e le associazioni del settore si svolgeranno delle iniziative volte a favorire la conoscenza del tema.

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.

Potenziali vittime dell'adescamento online possono essere sia bambini che bambine, sia ragazzi che ragazze. Il fenomeno, infatti, non conosce distinzione di genere. Gli adolescenti sono particolarmente vulnerabili, poiché si trovano in una fase della loro vita in cui è molto importante il processo di costruzione dell'identità sessuale. Anche per questo potrebbero essere aperti e curiosi verso nuove esperienze e, talvolta, attratti da relazioni intime e apparentemente rassicuranti. In questa fase è importante, infatti, il bisogno di avere attenzioni esclusive da un'altra persona, di ottenere rinforzi esterni di approvazione per il proprio corpo e la propria immagine. È proprio in ragione della fiducia costruita nella relazione che le vittime di adescamento online riferiscono di sentirsi umiliate, usate, tradite e tendono a sentirsi in colpa e ad autosvalutarsi per essere cadute nella trappola.

L'adescamento, quindi, non avviene apparentemente con una dinamica violenta, ma il "prendersi cura" del minore rappresenta la conditio per carpirne la fiducia ed instaurare una relazione a sfondo erotico. Può capitare che l'adescatore si presenti al minore sotto falsa identità, fingendo quindi di essere un'altra persona così da attirare maggiormente l'attenzione del minore (ad esempio, potrebbe fingersi un talent scout del mondo dello spettacolo alla ricerca di volti nuovi).

Ad oggi nella nostra scuola non si sono verificati casi di questa tipologia, tuttavia nelgli anni a venire anche in collaboazione con la psicologa della scuola, gli enti comprensoriali e le associazioni del settore si svolgeranno delle iniziative volte a favorire la conoscenza del tema. Verranno incentivate anche tutte le iniziative promosse dal territorio per aprondire le tematiche relative all'addescamento online.

4.7 - Pedopornografia

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

rappresentazione degli organi sessuali a fini soprattutto sessuali.

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

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

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

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

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

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

Il miglior modo per prevenire casi di adescamento online, che possono sfociare anche casi di pedoprornografia, è accompagnare ragazze e ragazzi in un percorso di educazione (anche digitale) all'affettività e alla sessualità. Ciò aiuterebbe a renderli 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. È molto importante, inoltre, che ragazzi e ragazze sappiano a chi rivolgersi in caso di problemi, anche quando pensano di aver fatto un errore, si vergognano o si sentono in colpa. Gli adulti coinvolti, genitori e docenti, devono essere un punto di riferimento per il minore che deve potersi fidare di loro e non sentirsi mai giudicato, ma compreso e ascoltato. Affinché ciò avvenga è necessario tenere sempre aperto un canale di comunicazione con loro sui temi dell'affettività, del digitale e perché no, della sessualità.

Nella società digitale, attraverso la Rete, i minori definiscono se stessi, si raccontano e sperimentano nuove forme di identità, socializzano, si emozionano e si relazionano con gli altri, scoprono la propria sessualità e giocano con essa.

Nel nostro istituto viene predisposto annualmente un percorso di educazione all'affettività e alle relazioni nella scuola primaria e nella secondaria di primo grado.

Il nostro piano d'azioni

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

Si propone il corso di Generazioni Connesse che contiene anche queste tematiche:

- la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai docenti e agli educatori.

Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/lle studenti/studentesse (Scuola Secondaria di primo Grado).

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

2020/2021 - 2021/2022

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

- 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, ai docenti e agli educatori, con il coinvolgimento di esperti.

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

- Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/lle studenti/studentesse (Scuola Secondaria di Primo Grado).

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.

Le Tecnologie dell'Informazione e della Comunicazione (TIC) sono parte integrante della vita quotidiana dei più giovani, in quanto strumenti privilegiati di comunicazione e di relazione, ma anche di informazione, studio, creatività e partecipazione, esse pongono però delle questioni associate alla "sicurezza" e al comportamento sociale. I rischi online rappresentano infatti tutte

quelle situazioni problematiche derivanti da un uso non responsabile delle tecnologie digitali da parte di bambini/e, ragazzi e ragazze. Per questo motivo gli insegnanti e gli educatori hanno il ruolo di guidare le attività on-line a scuola e illustrare le regole di comportamento per la navigazione in rete anche a casa.

I contenuti “pericolosi” per gli alunni possono essere i seguenti:

- contenuti che violino la privacy (foto personali, l'indirizzo di casa o il numero di telefono, informazioni private proprie o di amici, foto o video pubblicati contro la propria volontà, di eventi privati, ecc.);
- contenuti afferenti all’aggressività o alla violenza (messaggi minacciosi, commenti offensivi, pettegolezzi, informazioni false, foto o video imbarazzanti, virus, contenuti razzisti, che inneggiano al suicidio, immagini o video umilianti, insulti, videogiochi pensati per un pubblico adulto, ecc.);
- contenuti che implichino la sfera della sessualità.

Gli interventi che l'Istituto mette in atto sono perciò tesi a far conoscere e sensibilizzare gli alunni al fine di assicurare loro il rispetto del diritto ad essere tutelati da abusi e violenze da un lato e, allo stesso tempo, suscitare atteggiamenti di rispetto nei confronti degli altri utenti.

A questo scopo l'Istituto si attiva:

- per informare gli alunni dei rischi cui si espongono nella navigazione in rete;
- per limitare l'accesso a siti potenzialmente dannosi dotandosi di software che impediscono il collegamento ai siti web i cui contenuti possano risultare illegali o inadeguati (black list);
- consentendo l’utilizzo del cellulare solo per scopi didattici e sotto il controllo dei docenti e degli educatori;
- individuando un team preposto alla gestione della segnalazione (gestione interna alla scuola, invio ai soggetti competenti) ed un supporto psicologico interno alla scuola aperto alle studentesse e agli studenti, e ai loro genitori (sportello psicologico);
- prevedendo la collaborazione con enti, istituzioni e servizi presenti sul territorio a fronte di particolari e/o sistematiche situazioni di rischio.

5.2. - Come segnalare: quali strumenti e a chi

L'insegnante riveste la qualifica di pubblico ufficiale in quanto l'esercizio delle sue funzioni non è circoscritto all'ambito dell'apprendimento, ossia alla sola preparazione e tenuta delle lezioni, alla verifica/valutazione dei contenuti appresi dagli studenti e dalle studentesse, ma si estende a tutte le altre attività educative.

Le situazioni problematiche in relazione all'uso delle tecnologie digitali dovrebbero essere sempre gestite anche a livello di gruppo.

Come descritto nelle procedure di questa sezione, si potrebbero palesare due casi:

- CASO A (SOSPETTO) – Il docente ha il sospetto che stia avvenendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.
- CASO B (EVIDENZA) – Il docente ha evidenza certa che stia accadendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.

Per tutti i dettagli fate riferimento agli allegati con le procedure.

Strumenti a disposizione di studenti/esse

Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione:

- un indirizzo e-mail specifico per le segnalazioni;
- scatola/box per la raccolta di segnalazioni anonime da inserire in uno spazio accessibile e ben visibile della scuola;
- sportello di ascolto con professionisti;
- docente referente per le segnalazioni.

Anche studenti e studentesse, inoltre, possono rivolgersi alla Helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

Il nostro Istituto ha definito procedure per la rilevazione e la gestione dei problemi connessi ai comportamenti online a rischio di studenti e studentesse, così da indicare le modalità di presa in carico da parte della scuola e individuare l'intervento migliore da mettere in atto per aiutare gli studenti e le studentesse in difficoltà.

In relazione ai rischi collegati alle TIC, i docenti ed il personale scolastico sono tenuti a vigilare e a rilevare eventuali situazioni di criticità. Alcune situazioni di disagio vissute dagli studenti/studentesse possono emergere attraverso:

- osservazione sistematica da parte dei docenti e degli educatori nelle classi;
- richieste specifiche ai ragazzi sul loro benessere all'interno e all'esterno della scuola, anche non necessariamente in situazione di palese disagio, e ascolto attento di quanto eventualmente raccontano;
- punto di raccolta segnalazioni di disagio (box) da parte degli alunni/e attraverso l'utilizzo di una cassetta (oppure casella di posta elettronica) in cui inserire delle comunicazioni, contenenti nome, cognome, classe, data ed una breve descrizione del fatto che causa disagio;
- sportello di ascolto con psicologa della scuola;
- docente e/o educatore referente per le segnalazioni.

Sia nel caso di sospetto che nel caso di evidenza che un/a studente/essa possa essere vittima o responsabile di una situazione di disagio connessa a cyberbullismo, sexting o adescamento online, i docenti, gli educatori e il personale scolastico dovranno informare il Responsabile per il cyberbullismo e il Dirigente scolastico utilizzando la scheda di segnalazione allegata.

Il Dirigente Scolastico contatterà il docente e/o l'educatore e/o il personale scolastico per un colloquio finalizzato all'analisi della situazione ed alle azioni da intraprendere, anche avvalendosi del supporto ed alla consulenza della psicologa della scuola.

Il Responsabile attiverà le procedure interne ed eventualmente con le istituzioni preposte, secondo i protocolli suggeriti dalla piattaforma messa a disposizione da "Generazioni Connesse" e allegati al presente documento. Se necessario, si coinvolgerà la famiglia.

Tutte le segnalazioni dei docenti devono essere protocollate e messe a verbale.

Alcuni avvenimenti di lieve rilevanza possono essere affrontati e risolti con la discussione collettiva in classe. Altri casi possono essere affrontati con la convocazione di genitori e alunni, alla presenza del Referente del Cyberbullismo e della psicologa di Istituto, per riflettere insieme sull' accaduto e individuare strategie comuni d'intervento.

Nei casi più gravi e in ogni ipotesi di reato, occorre valutare tempestivamente con il Dirigente Scolastico come intervenire, convocando con urgenza i genitori.

Per i reati più gravi (es. pedopornografia) gli operatori scolastici hanno l'obbligo di effettuare la denuncia all'autorità giudiziaria (o più semplicemente agli organi di polizia territorialmente

competenti). In particolare per i fatti criminosi, ai fini della denuncia ,la relazione deve essere redatta nel modo più accurato possibile.

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.

Le procedure individuate sono comunicate e condivise con l'intera comunità scolastica attraverso le assemblee scolastiche che coinvolgono i genitori, gli studenti e le studentesse e il personale della scuola, attraverso news nel sito della scuola e durante i collegi docenti.

A seguire le problematiche a cui fanno riferimento le azioni previste, che possono essere pianificate anche a livello preventivo.

RISCHI	AZIONI
Adescamento online (grooming)	Sensibilizzazione sull'esistenza di individui che usano la rete per instaurare relazioni, virtuali o reali, con minorenni e per indurli alla prostituzione. Qualora si venga a conoscenza di casi simili, occorre valutarne la fondatezza e avvisare tempestivamente il Referente di Istituto per il cyberbullismo ed il Dirigente scolastico.
Cyberbullismo	Creazione di spazi in cui gli alunni si possano confrontare su questo tema, utilizzando come spunti di riflessione: spezzoni di film, canzoni, materiali prodotti da altri alunni coinvolti nel progetto SIC. Campagne di sensibilizzazione e informazione anche con l'ausilio di progetti e realtà esterni e con l'utilizzo dei materiali disponibili su "Generazioni connesse". I casi possono essere molto variegati, andando dal semplice scherzo di cattivo gusto via sms/Whatsapp a vere e proprie minacce verbali e fisiche, che costituiscono reato. Occorre confrontarsi con il Referente e/o con il Dirigente Scolastico sulle azioni da intraprendere che coinvolgeranno anche il Consiglio di classe.
Dipendenza da Internet videogiochi, shopping o gambling online	Informazioni sul fatto che ciò può rappresentare una vera e propria patologia che compromette la salute e le relazioni sociali e che in taluni casi (per es. uso della carta di credito a insaputa di altri) rappresenta un vero e proprio illecito. Divieto per gli alunni di utilizzare propri dispositivi digitali in classe ad eccezione di specifiche e regolamentate attività didattiche. Qualora si venga a conoscenza di casi simili, occorre convocare i genitori per invitarli a un maggiore controllo sulla fruizione di internet da parte dei propri figli e/o sulla necessità di non usufruirne in presenza degli stessi.
Esposizione a contenuti pornografici, violenti, razzisti	Verso i genitori: informazione circa le possibilità di attivare forme di controllo parentale della navigazione e sensibilizzazione sulla necessità di monitorare l'esperienza online dei propri figli. Verso la componente studentesca: inserimento nel curricolo di temi legati alla affidabilità delle fonti online, all'interculturalità e al rispetto delle diversità. Qualora si venga a conoscenza di casi simili, occorre convocare i genitori per invitarli a un maggiore controllo sulla fruizione di internet da parte dei propri figli e/o sulla necessità di non usufruirne in presenza degli stessi.

Sexting e pedopornografia	Verso i genitori: informazione circa le possibilità di attivare forme di controllo parentale della navigazione. Verso la componente studentesca: inserimento nel curricolo di temi legati all'affettività, alla sessualità e alle differenze di genere. In casi simili, se l'entità è lieve occorre in primo luogo parlarne con alunne e alunni e rispettivi genitori, ricordando loro che l'invio e la detenzione di foto che ritraggono minorenni in pose sessualmente esplicite configura il reato di distribuzione di materiale pedopornografico. Manca spesso la consapevolezza, tra ragazzi e adulti, che una foto o un video diffusi in rete divengono di pubblico dominio e la diffusione non è controllabile. In casi di rilevante gravità occorre informare tempestivamente il Dirigente Scolastico e va coinvolto il Referente per il Cyberbullismo per l'attivazione di specifiche procedure.
Violazione della privacy	Informazione sull'esistenza di leggi in materia di tutela dei dati personali e di organismi per farle rispettare. Se il comportamento rilevato viola solo le norme di buona convivenza civile e di opportunità, occorre convocare i soggetti interessati per informarli e discutere dell'accaduto e concordare forme costruttive ed educative di riparazione. Qualora il comportamento rappresenti un vero e proprio illecito, il Dirigente Scolastico deve esserne informato in quanto a seconda dell'illecito sono previste sanzioni amministrative o penali.

Sono inoltre attivi 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.

5.3. - 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

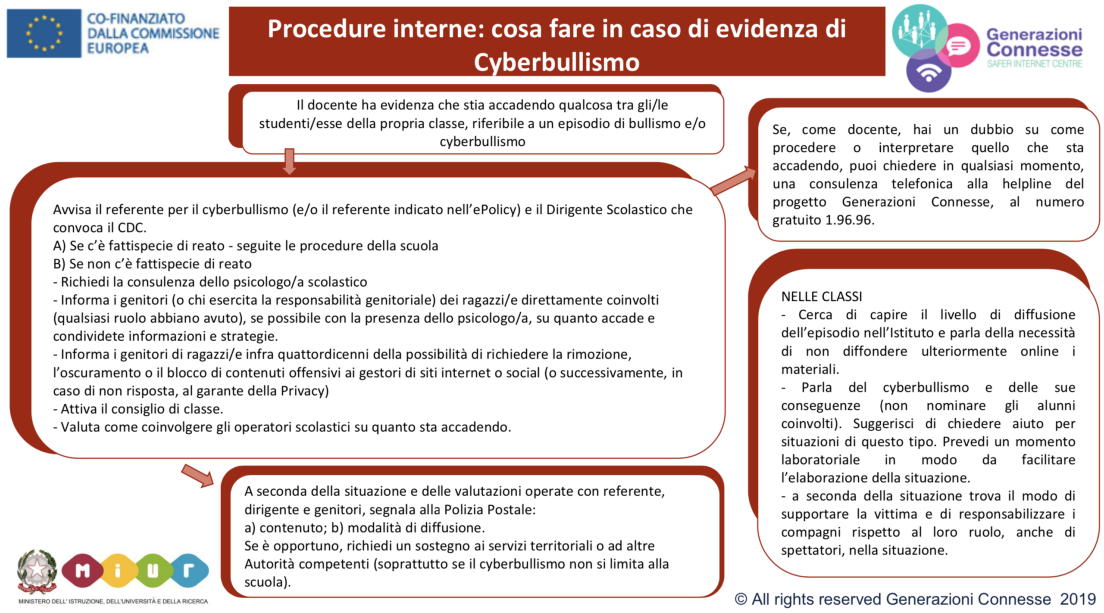
difensore dei diritti dell'infanzia.

- **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.

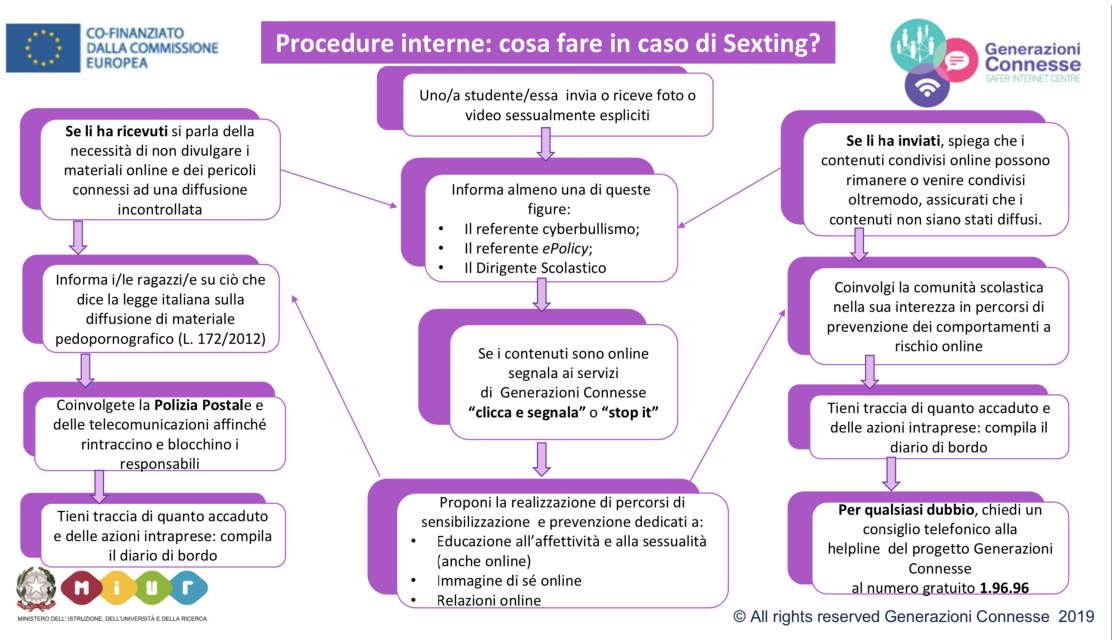
Nell'affrontare i casi di sospetto/certezza di rischio, e qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze o richiedano un intervento specifico, la scuola prevede la collaborazione con enti, istituzioni e servizi presenti sul territorio.

5.4. - Allegati con le procedure

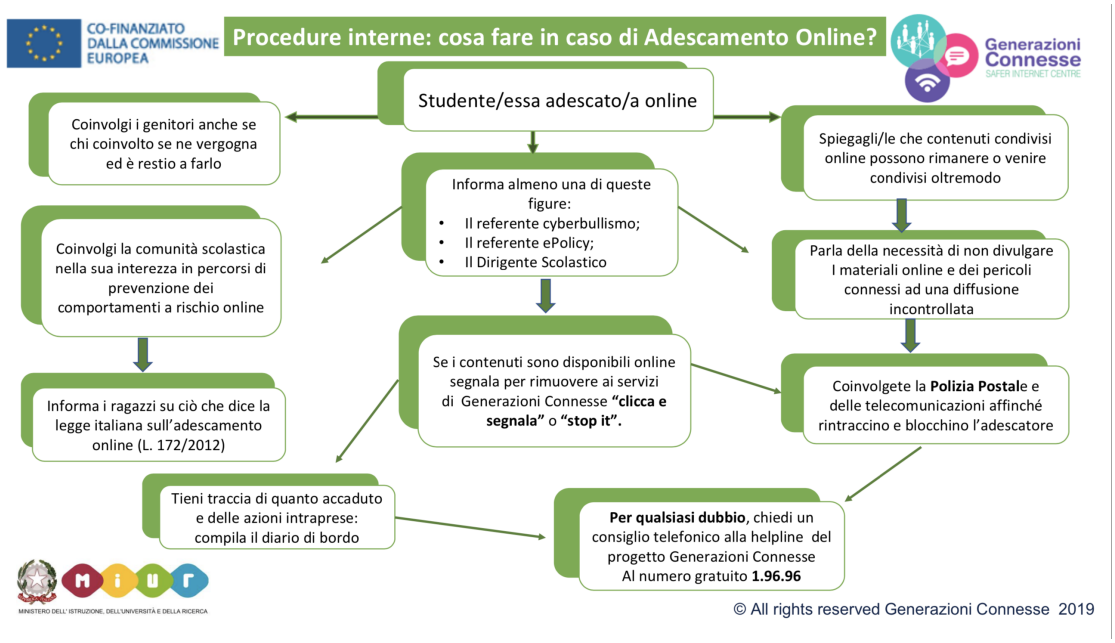
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



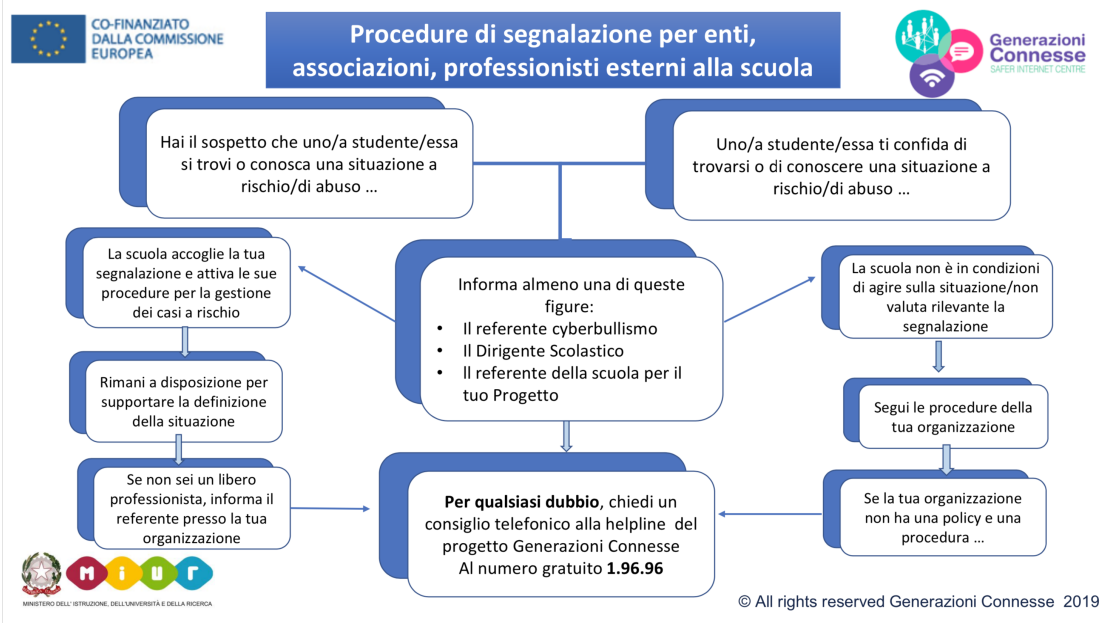
Procedure interne: cosa fare in caso di sexting?



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

2020/2021

- Elabora una scheda di rilevazione delle criticità/disagi rivolta agli studenti e alle studentesse dalla classe V primaria alla V liceo.
- La scuola individua il team preposto alla gestione della segnalazione.

- Elabora azioni specifiche da inserire nel curricolo al fine di sensibilizzare gli alunni sui temi del cyberbullismo anche utilizzando materiale di Generazioni connesse.

- Intraprende un percorso di armonizzazione tra documento ePolicy/Patto corresponsabilità - Regolamento Istituto/PTOF.