Documento di ePolicy

SOIC80500D

I.C. BERTACCHI - CHIAVENNA

PIAZZA DON PIETRO BORMETTI 3 - 23022 - CHIAVENNA - SONDRIO (SO)

Eliana Giletti

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.

Tali priorità sono state rese ancora più impellenti in seguito all'implementazione della Didattica a distanza (DaD) durante il lockdown per l'emergenza sanitaria e alla necessità di utilizzare le nuove

tecnologie per la Didattica Digitale Integrata per offrire ai nostri studenti e alle nostre studentesse l'occasione di ampliare il loro apprendimento tramite le tecnologie che impareranno a utilizzare in maniera appropriata.

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.

Tutti i soggetti coinvolti sono responsabili dell'uso che fanno delle tecnologie, ma individuiamo alcune figure di riferimento che possono affiancare docenti, studenti, personale e famiglie nel loro percorso di acquisizione di una maggiore consapevolezza e di crescita nella Cittadinanza digitale.

1. **Dirigente Scolastico**

Si occupa di monitorare le situazioni che vengono segnalate dagli insegnanti referenti.
Ha la responsabilità di far sì che l'Istituto si doti degli opportuni sistemi per un uso sicuro delle TIC ed in particolare di Internet; se necessario trova i finanziamenti per l'acquisto di apposito software o per la formazione degli alunni e di altri soggetti interessati.

2. **Animatore digitale**

Il nostro istituto è dotato di un insegnante che stimola la formazione interna negli ambiti di sviluppo della "scuola digitale".
In particolare tale figura promuove iniziative per la diffusione dell'educazione alla sicurezza online come cardine nello sviluppo delle competenze digitali (educazione alla cittadinanza digitale) e affianca i docenti che educano alla sicurezza online nello svolgersi del curriculum della propria disciplina. Essa inoltre ha il compito di monitorare e rilevare le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola, nonché proporre la revisione delle politiche dell'istituzione con l'individuazione di soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola.

3. **Referente per il contrasto di bullismo e cyberbullismo**

Ha il compito di promuovere iniziative per la diffusione dell'educazione alla sicurezza online in relazione al corretto utilizzo delle tecnologie della comunicazione, con particolare attenzione alle modalità di comunicazione e alla protezione dei soggetti più fragili e a rischio.

4. **Team digitale**

Si affianca all'animatore digitale per favorire la diffusione dell'educazione alla sicurezza online.

5. **Psicopedagogista d'Istituto**

Nell'ambito dello sportello di ascolto attivato nell'Istituto, si occupa di sostenere alunni, genitori e insegnanti nella gestione di comportamenti a rischio per quanto di sua competenza.

6. **Rappresentante dei genitori**

Sarà individuato tra i genitori degli alunni della scuola secondaria e delle classi quarta e quinta primaria, per coordinare i rapporti tra i genitori e le figure suindicate e per favorire la diffusione di una cultura digitale e del corretto uso della tecnologia.

7. **Rappresentante degli alunni**

Si valuterà la possibilità di individuare tra gli alunni delle classi terminali della scuola secondaria di primo grado dei responsabili che possano affiancare i compagni nell'ottica della peer education.

8. **Alunni dei diversi ordini di scuola (in particolare della Scuola secondaria di 1^ grado)**

Devono conoscere i contenuti della presente Policy e dei regolamenti ad essa allegati e chiarire eventuali dubbi con le figure di riferimento.
● Assumono comportamenti improntati alla sicurezza e alla responsabilità nel loro uso delle tecnologie dentro e fuori la scuola.
● Comprendono che la segnalazione di comportamenti scorretti (uso improprio, accesso a contenuti inappropriati e assunzione di rischi) è un dovere civile e non è scorretto nei confronti del compagno che sbaglia.

9. **Inoltre, tutto il personale dell'istituto, gli educatori, gli esperti esterni, i volontari e ogni persona che a qualsiasi titolo interagisce con gli alunni nella scuola sono tenuti a:**

● conoscere i contenuti della presente Policy e dei regolamenti ad essa allegati e chiarire eventuali dubbi con le figure di riferimento;
● segnalare qualsiasi comportamento sospetto, sia esso abuso o rischio alla Dirigente o alle figure referenti di cui ai punti precedenti;
● assumere comportamenti sicuri, responsabili e professionali nell'uso delle tecnologie così da comunicare con il buon esempio agli alunni.

10. **Genitori**

● Devono conoscere i contenuti della presente Policy e dei regolamenti ad essa allegati (eventualmente chiarendo eventuali dubbi con le figure di riferimento) per poter affiancare i propri figli nel loro percorso di maturazione nell'utilizzo consapevole delle tecnologie.
● Sono invitati a segnalare comportamenti devianti o comunque per loro preoccupanti alle figure di riferimento.

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).

Si invitano quindi i soggetti che a qualsiasi titolo si trovino a interagire con gli studenti e le studentesse nel contesto scolastico a prendere visione del documento e delle regole in esso contenuto per applicarle nelle loro relazioni all'interno 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 garantirne la massima diffusione esso viene allegato al Piano Triennale dell'Offerta Formativa.
Viene condiviso con i docenti e il personale attraverso il cloud d'Istituto.
Viene inviata comunicazione del suo aggiornamento ai genitori tramite Registro Elettronico; per i genitori potrà essere previsto un incontro di presentazione in occasione dell'inizio del percorso scolastico dei figli all'interno dell'Istituto.

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 allegherà al presente documento una lista delle infrazioni più comuni per far sì che gli studenti e le studentesse possano evitare di commetterle. Le sanzioni saranno sempre temporanee, commisurate alla gravità dell'infrazione e ispirate al principio della gradualità e, quando possibile, della riparazione del danno. Esse infatti hanno finalità educative e si propongono di rafforzare il senso di responsabilità del singolo.

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.

La presente ePolicy tiene comunque conto dei Regolamenti già deliberati dal Collegio Docenti e dal Consiglio di Istituto negli anni precedenti e rimanda ad essi per maggiori dettagli in riferimento ad alcuni comportamenti (per esempio il corretto utilizzo dei propri dispositivi durante la didattica - BYOD policy).

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.

Tale efficacia potrà essere valutata nel corso della compilazione del Rapporto di AutoValutazione dell'Istituto, nonché attraverso questionari compilati da tutti gli attori coinvolti (personale, alunni e famiglie).

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i docenti dell'Istituto per la stesura finale dell'ePolicy.
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse e dell'ePolicy rivolto agli studenti
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse e dell'ePolicy rivolto ai genitori

Azioni da svolgere nei prossimi 3 anni:

- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i genitori dell'Istituto per l'aggiornamento dell'ePolicy.
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse e dell'ePolicy rivolto ai docenti
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai genitori dei nuovi alunni
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto agli alunni

delle classi terminali della scuola primaria

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.

E' prevista la stesura di un curricolo digitale nel corso dell'anno scolastico 2020/21 e l'implementazione dello stesso a partire dal successivo anno scolastico. Nel frattempo comunque tutti gli alunni delle classi quarta e quinta e alcuni alunni delle altre classi della scuola primaria (compatibilmente con le risorse a disposizione della scuola e con le valutazioni didattiche delle insegnanti) vengono formati al corretto uso delle piattaforme utilizzate durante la Didattica Digitale Integrata.

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

nella didattica

È fondamentale che i docenti tutti siano formati ed aggiornati sull'uso corretto, efficace ed efficiente delle TIC nella didattica, al fine di usarle in modo integrativo ed inclusivo.

Ciò si rende necessario per fornire agli studenti e alle studentesse modelli di utilizzo positivo, critico e specifico delle nuove tecnologie e per armonizzare gli apprendimenti.

Il nostro Istituto negli ultimi anni ha provveduto ad avviare una formazione specifica relativa all'uso delle nuove tecnologie nella didattica (LIM e piattaforma GSuite), a promuovere l'utilizzo di spazi cloud d'Istituto per la condivisione di attività e la diffusione delle buone pratiche (Gsuite for Education) e all'introduzione del registro elettronico (azione #12) nella scuola primaria e secondaria di primo grado. Si prevede inoltre per l'anno scolastico 2020/21 che tutti i docenti della scuola primaria seguano il corso organizzato per l'utilizzo della piattaforma GSuite nella Didattica a Distanza.

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

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

Tali incontri si sostanzieranno in momenti di interazione online e condivisione di tutorial con gli insegnanti per permettere loro di approfondire le proprie conoscenze in merito alle tematiche appena esposte.

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.

Si prevede inoltre di mettere in campo delle specifiche iniziative formative a distanza anche a seguito di consultazione sulle esigenze espresse dalle famiglie.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2020/2021)

- Effettuare un'analisi del fabbisogno formativo del corpo docente 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.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare incontri con esperti per i docenti sulle competenze digitali.

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

- Coinvolgere una rappresentanza dei genitori per individuare i temi di maggiore interesse nell'ambito dell'educazione alla cittadinanza digitale.
- Organizzare incontri con esperti per i docenti sulle competenze 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.

La nostra scuola si avvale della consulenza di un esperto esterno che aiuta i responsabili a valutare le corrette azioni da implementare per rispondere alle richieste della legge in materia di protezione della privacy.

Per quanto riguarda l'utilizzo delle nuove tecnologie si sottolinea come i dati raccolti attraverso l'accesso alla piattaforma siano solo nome e cognome dell'alunno e che eventuali dati sensibili associati agli stessi e trattati elettronicamente sono gestiti in maniera da tutelarne il diritto alla riservatezza.

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.

A tal proposito il nostro Istituto si impegna a collaborare con i Sindaci e gli altri rappresentanti dei comuni sede dei nostri plessi scolastici per dotare tutte le sedi di un'adeguata connessione a Internet e a potenziare la stessa ove non fosse sufficiente a soddisfare i bisogni legati alla Didattica Digitale Integrata e all'utilizzo delle TIC in classe, in particolare nella scuola secondaria di primo grado.

La scuola sta lavorando anche per acquisire i dispositivi necessari a fornire la possibilità di connessione anche agli studenti e alle studentesse privi di mezzi propri.

3.3 - Strumenti di comunicazione online

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

Il nostro Istituto fornisce agli studenti e alle studentesse un account GSuite istituzionale nel formato cognomenome@icbertacchi.edu.it, tramite il quale gli alunni hanno accesso alla posta elettronica per comunicare con gli insegnanti (non sono consentite comunicazione con indirizzi esterni da parte degli alunni), alle classi virtuali tramite Classroom e alla gestione di documenti nel cloud tramite Google Drive. Tali app consentono di lavorare collaborativamente anche a distanza e di ampliare quindi le occasioni di interazione tra gli studenti in un'ottica di apprendimento cooperativo e di peer education. La possibilità di un canale di comunicazione integrativo rispetto alla didattica in presenza consente anche agli studenti più timidi di porre i propri quesiti all'insegnante e di risolvere eventuali dubbi senza esporsi all'imbarazzo che possono provare di fronte al resto della classe.

Tale comunicazione tra studenti e docenti facilita anche la personalizzazione e l'individualizzazione degli apprendimenti in un'ottica di maggiore inclusività dell'azione didattica.

3.4 - Strumentazione personale

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

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

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

Per strumentazione personale si intendono telefoni cellulari, tablet, fotocamere, registratori vocali e qualsiasi dispositivo tecnologico atto alla comunicazione con l'esterno e alla registrazione di audio e video.

1. **Guida all'uso per gli studenti**

Come da regolamento BYOD (link) essi possono essere utilizzati durante le lezioni scolastiche solo se previsto dall'attività didattica e secondo specifiche modalità concordate con l'insegnante responsabile.
Nella scuola primaria si chiede alle famiglie di non far portare di norma tali dispositivi ad alunne e alunni, tranne che nei casi in cui viene esplicitamente richiesto di portare un tablet; nella scuola secondaria di primo grado tali dispositivi se portati con sé saranno spenti all'ingresso in aula ed eventualmente accesi come da regolamento BYOD.
L'utilizzo per gli alunni con BES/DSA, sarà concordato con le famiglie ed esplicitato nel relativo PDP redatto dal Consiglio di Classe.
Non è consentito l'uso di console portatili quali Playstation, Nintendo Switch e similari, anche in ragione del loro accesso a Internet non filtrato.
Si sottolinea che l'invio di materiali abusivi, offensivi o inappropriati è vietato, anche se avviene all'interno di cerchie o gruppi di discussione privati.
Il docente che ravvisi un'infrazione a quanto sopra riportato consegnerà l'apparecchio requisito alla segreteria, dove i genitori convocati potranno recuperarlo e informarsi in merito ad eventuali sanzioni comminate.
In caso di urgenti necessità di comunicazione con la famiglia durante l'orario scolastico, alunne e alunni possono usare gratuitamente la linea fissa della scuola rivolgendosi a un collaboratore scolastico - si ricorda che alla scuola secondaria di primo grado gli alunni dovrebbero essere responsabilizzati in merito ad eventuali dimenticanze e quindi questa non rappresenta un'urgenza; allo stesso modo le famiglie possono comunicare con i propri figli chiamando la segreteria. Si raccomanda di ridurre tali comunicazioni a casi di inderogabile necessità e urgenza.

2. **Guida all'uso per i docenti**

Quando possibile il personale docente utilizzerà la strumentazione messa a disposizione dalla scuola, per tutti gli scopi connessi alla didattica. E' possibile utilizzare telefoni cellulari, tablet, fotocamere e altri strumenti di registrazione audio/video solo per attività didattiche, anche per dare il corretto esempio agli alunni. In casi di emergenza, qualora non fosse possibile contattare di persona un collaboratore scolastico, gli insegnanti sono autorizzati a utilizzare il proprio telefono cellulare. La password di accesso alla rete wireless e ai computer di classe (soprattutto nella scuola secondaria di primo grado) va custodita con cura e non comunicata a terzi: si ricorda che per quel che riguarda la sede centrale della secondaria l'uso improprio sarà verificabile in seguito all'aggiornamento della rete wifi. Qualora si utilizzino a scuola dispositivi di archiviazione esterna di proprietà personale (chiavette usb, dischi fissi portatili) è bene controllare preventivamente che essi siano esenti da virus per evitare di danneggiare le attrezzature comuni.
Durante la didattica è opportuno che ogni insegnante indichi chiaramente in cosa consiste il corretto utilizzo della rete per quell'attività, ricordando agli studenti la relativa netiquette.
Come è già consuetudine all'interno dell'Istituto il docente è tenuto a segnalare prontamente eventuali malfunzionamenti o danneggiamenti al responsabile per l'informatico.

3. **Guida all'uso per altre figure professionali**

Gli educatori professionali seguiranno il regolamento di cui sopra e le indicazioni dell'insegnante responsabile della classe in cui si trovano ad operare.
I collaboratori scolastici utilizzeranno se necessario le apparecchiature della scuola e seguiranno le indicazioni della Direttiva MIUR n°104 del 15 marzo 2007 in merito all'utilizzo dei cellulari ed altre apparecchiature.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2020/2021).

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli studenti e delle studentesse della scuola secondaria
- 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 genitori degli studenti e delle 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).

- Organizzare uno o più eventi o attività volti a consultare i docenti dell'Istituto per aggiornare se necessario i regolamenti sull'uso dei dispositivi digitali personali.
- Organizzare incontri per la consultazione dei genitori su indicazioni per

l'aggiornamento dei regolamenti sull'uso dei dispositivi digitali personali

- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare 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'individuazione dei rischi connessi all'utilizzo delle nuove tecnologie sarà sottoposta a continue revisioni e aggiornamenti in relazione alla velocità con cui si evolvono le TIC.
In particolare si ricordano qui alcuni dei principali rischi a cui fare attenzione, senza alcuna pretesa di esaustività:

- Cyberbullismo
- Comunicazioni inappropriate con adulti
- Condivisione di materiale pedopornografico
- Download di virus e ransomware

- Dipendenza patologica da Internet, giochi online (ludopatie)
- Esposizione a contenuti violenti e di natura razzista, omofoba, sessista
- Violazione della privacy
- Violazione del diritto d'autore ed eventuali sanzioni di legge

1. **Azioni di sensibilizzazione**

Si organizzeranno degli incontri di sensibilizzazione con le famiglie e gli alunni, nonché degli specifici momenti nella didattica, soprattutto per le classi terminali della scuola primaria e per gli alunni della scuola secondaria di primo grado per identificare i rischi più probabili in relazione alle diverse fasce d'età e per individuare i possibili comportamenti protettivi per sé e per gli altri.
Sarà possibile anche realizzare delle UDA che portino alla produzione di materiali di comunicazione di diversa natura (testi, poster, prodotti multimediali, ecc.) in merito ai rischi di cui sopra - in generale o in relazione al singolo elemento.

2. **Azioni di prevenzione**

Per prevenire comportamenti scorretti online, l'Istituto propone a partire dall'anno scolastico 2021/22, l'implementazione di un curricolo digitale in tutte le classi della scuola primaria e secondaria. Si condivide comunque a livello di tutto l'Istituto una serie di pratiche (netiquette) che favoriscano corretti rapporti online. Nella scuola secondaria di primo grado è normalmente attivo uno sportello di ascolto gestito dalla psicopedagogista, che è disponibile ad affiancare gli alunni e gli insegnanti anche nella gestione di comportamenti a rischio.
Tale sportello è momentaneamente sospeso nella sua realizzazione in presenza durante l'emergenza sanitaria.

Negli anni passati sono stati previsti anche degli incontri sulla prevenzione dell'abuso nelle classi quarte della primaria (Progetto Porcospini) e per il corretto approccio alle nuove tecnologie nelle classi prime della scuola secondaria di primo grado (Progetto Whatsapp). Ci si propone di riprenderli una volta usciti dall'emergenza.

L'Istituto inoltre ha aderito al Progetto "Life Skills Training", che ha lo scopo di promuovere il benessere e la salute degli alunni anche in relazione alla prevenzione delle ludopatie.

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).

Data la natura particolarmente elusiva delle azioni di cyberbullismo, che spesso vengono inflitte tramite alias che sembrano garantire ai perpetratori un presunto anonimato, si richiama la necessità di azioni di collaborazione tra le famiglie e la comunità educante tutta per individuare e prevenire eventuali episodi di cyberbullismo. L'Istituto ha già adottato un modulo di segnalazione online disponibile sulla sezione del sito dedicata alla prevenzione di bullismo e cyberbullismo (link). Ci si propone di raccogliere proposte in merito a canali alternativi per facilitare il più possibile la raccolta delle segnalazioni.

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

Il fenomeno di "incitamento all'odio" o "discorso d'odio", indica discorsi (post, immagini, commenti etc.) e pratiche (non solo online) che esprimono odio e intolleranza verso un gruppo o una persona (identificate come appartenente a un gruppo o categoria) e che rischiano di provocare reazioni violente, a catena. Più ampiamente il termine "hate speech" indica un'offesa fondata su una qualsiasi discriminazione (razziale, etnica, religiosa, di genere o di orientamento sessuale, di

disabilità, eccetera) ai danni di una persona o di un gruppo.

Tale fenomeno, purtroppo, è sempre più diffuso ed estremamente importante affrontarlo anche a livello educativo e scolastico con l'obiettivo di:

- fornire agli studenti gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di hate speech, in particolare legati alla razza, al genere, all'orientamento sessuale, alla disabilità;
- promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network;
- favorire una presa di parola consapevole e costruttiva da parte dei giovani.

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere in relazione a questa problematica.

- Si prevede di inserire delle lezioni in merito a questa tematica nel curricolo di Istituto di Educazione Civica.
- I docenti monitorano gli atteggiamenti degli studenti e implementano le necessarie azioni educative quando gli studenti siano impegnati in attività riconducibili all'Hate speech.
- Tutto il personale della scuola si impegna ad adottare un comportamento rispettoso delle diversità e a evitare qualsiasi forma di Hate speech nella propria comunicazione in classe e nelle situazioni in cui si esprime in veste professionale.

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?

L'Istituto ha aderito al Progetto "Life Skills Training", che ha lo scopo di promuovere il benessere e la salute degli alunni anche in relazione alla prevenzione delle ludopatie.

Inoltre alcuni insegnanti della scuola secondaria di primo grado hanno frequentato un apposito corso di formazione e sono in grado di affrontare questa tematica in classe.

Naturalmente si ritiene della massima importanza promuovere un utilizzo positivo e benefico delle tecnologie in tutti gli ordini di scuola ed è quindi importante monitorare il rapporto con le stesse in tutti gli ordini di scuola per prevenire sin dagli alunni più giovani eventuali forme di abuso o di uso scorretto della tecnologia.

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.

Per prevenire tali rischi gli insegnanti si impegnano a sottolineare con gli alunni l'importanza del rispetto della privacy altrui e richiamano gli stessi a condividere immagini dei compagni solo se espressamente autorizzati dagli stessi.

Naturalmente data la giovane età degli alunni si utilizzerà un linguaggio adeguato e comprensibile e si condivideranno solo le informazioni appropriate in relazione all'età dei destinatari.

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.

Nell'Istituto già da diversi anni le classi quarte della scuola primaria sono destinatarie di un intervento di prevenzione legato al "Progetto Porcospini" erogato da personale qualificato. Tale progetto ha lo scopo di prevenire eventuali situazioni di adescamento e abuso dei minori e si ritiene

quindi una valida iniziativa da proporre agli alunni.

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.

Gli insegnanti si propongono sempre di tutelare il benessere psico-fisico dei propri alunni e qualora dovessero notare dei comportamenti anomali lo segnaleranno alla famiglia e alla Dirigente, per permettere di verificare quanto effettivamente accaduto e l'eventuale necessità di un supporto psicologico per i bambini e le bambine esposti a immagini e altro materiale non adatto alla loro età.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2020/2021).

□ Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse, se possibile anche 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, se possibile con il coinvolgimento di esperti.

□ Organizzare uno o più incontri di formazione all'utilizzo sicuro e consapevole di Internet e delle tecnologie digitali integrando lo svolgimento della didattica e assicurando la partecipazione attiva degli studenti/studentesse.

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

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

□ Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse, se possibile anche 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, se possibile con il coinvolgimento di esperti.

□ Organizzare uno o più incontri di formazione all'utilizzo sicuro e consapevole di Internet e delle tecnologie digitali integrando lo svolgimento della didattica e assicurando la partecipazione attiva degli studenti/studentesse.

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

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

☐ Organizzare uno o più eventi e/o dibattiti in momenti extra-scolastici, sui temi della diversità e sull'inclusione rivolti a genitori, studenti/studentesse e personale della scuola.

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

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.

Insegnanti, alunni, famiglie e personale della scuola sono invitati a segnalare eventuali comportamenti a rischio di cui fossero testimoni o di cui venissero a conoscenza (in particolare da parte degli alunni) secondo le modalità sottoindicate.

1. Modulo online

Sulla sezione del nostro sito dedicata alla prevenzione del bullismo e del cyberbullismo reperibile al seguente link: https://sites.google.com/icbertacchi.edu.it/no-bullismo-bertacchi/in-evidenza/modulo. Attraverso tale strumento sarà possibile, anche in forma anonima, segnalare eventuali episodi riconducibili a atti di bullismo o cyberbullismo. ll referente per la prevenzione di bullismo e cyberbullismo si occuperà poi di riportare tale segnalazione alla Dirigente che si occuperà di raccogliere tutte le informazioni utili a chiarire la dinamica di quanto accaduto per accertare eventuali responsabilità.

2. Incontro con Dirigente e/o referente

I genitori o i docenti che volessero segnalare eventuali episodi di bullismo o cyberbullismo possono prendere appuntamento con la Dirigente e/o la referente d'Istituto per riportare le informazioni in loro possesso e consentire quindi di avviare le necessarie indagini interne per accertare l'accaduto.

3. Colloquio con docente

Gli alunni possono rapportarsi anche con i docenti per segnalare eventuali episodi di bullismo e cyberbullismo. Saranno poi i docenti a contattare la Dirigente e/o la referente per la prevenzione di bullismo e cyberbullismo per riferire quanto appreso riportando tutte le informazioni utili per comprendere l'accaduto.

Sarà cura della Dirigente contattare eventualmente l'alunno/a e/o la sua famiglia per eventuali approfondimenti.

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.

Si riporta qui l'indirizzo email del referente per bullismo e cyberbullismo per eventuali segnalazioni: prevenzione-bullismo@icbertacchi.edu.it.

Gli alunni possono inoltre utilizzare la scatola dello Sportello No Problem per inserire eventuali segnalazioni oltre che prenotare un colloquio con la psicopedagogista.

Si specificano qui le procedure da seguire nei casi di sospetto (A) o di certezza (B) di episodi di bullismo/cyberbullismo, sexting o adescamento online.

- Nel CASO A (SOSPETTO) – Il docente raccoglie tutte le informazioni che riesce e osserva (eventualmente coinvolgendo anche il Team o il Consiglio di classe) tutti gli elementi utili per decidere se procedere con la segnalazione oppure se si tratta di un falso allarme. In caso di dubbio si confronta con la Dirigente e/o il referente per la prevenzione di bullismo e cyberbullismo. In seguito a questo colloquio si deciderà se raccogliere ulteriori elementi oppure se non è necessario e allora si prospettano due scenari: nel primo caso l'episodio non è riconducibile ad episodi di bullismo e/o cyberbullismo, sexting o adescamento online e allora viene steso un breve verbale di quanto discusso da allegare al fascicolo dell'alunno/a; nel secondo caso invece vengono raccolte delle evidenze e si fa riferimento al caso successivo.
- CASO B (EVIDENZA) – Il docente ha evidenza certa, per esempio testimonianza diretta della vittima o di qualcuno che ha assistito oppure filmati, immagini o prove scritte di quanto avvenuto. In questo caso riporta tali elementi alla Dirigente che si occuperà, in caso di reati,

di coinvolgere le autorià competenti. Nel caso in cui gli episodi non si configurassero come reato sarà compito del Team/Consiglio di classe individuare eventuali interventi e/o sanzioni (se gli episodi si sono verificati in classe o sono comunque di gravità rilevante).

5.3. - Gli attori sul territorio

Talvolta, nella gestione dei casi, può essere necessario rivolgersi **ad altre figure, enti, istituzioni e servizi presenti sul territorio** qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.

Per una mappatura degli indirizzi di tali strutture è possibile consultare il Vademecum di Generazioni Connesse "Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all'utilizzo delle tecnologie digitali da parte dei più giovani" (seconda parte, pag. 31), senza dimenticare che la Helpline di Telefono Azzurro (19696) è sempre attiva nell'offrire una guida competente ed un supporto in tale percorso.

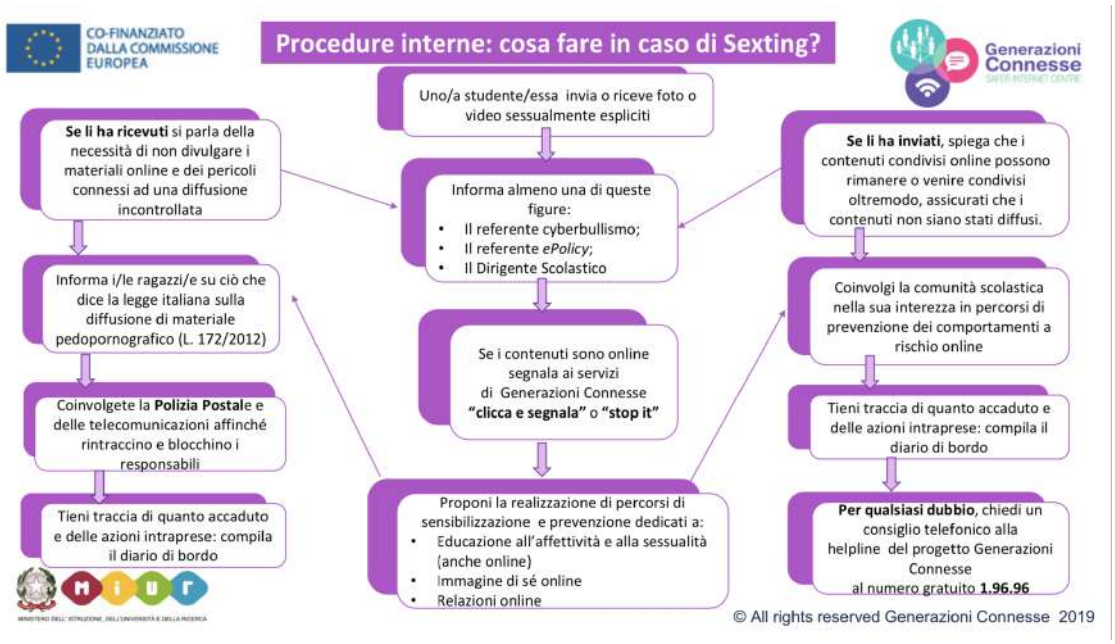
A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all'utilizzo di Internet può presentare.

- **Comitato Regionale Unicef**: laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni)**: svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare attenzione alla tutela dei minori.
- **Ufficio Scolastico Regionale**: supporta le scuole in attività di prevenzione ed anche nella segnalazione di comportamenti a rischio correlati all'uso di Internet.
- **Polizia Postale e delle Comunicazioni**: accoglie tutte le segnalazioni relative a comportamenti a rischio nell'utilizzo della Rete e che includono gli estremi del reato.
- **Aziende Sanitarie Locali**: forniscono supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in Rete. In alcune regioni, come il Lazio e la Lombardia, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da Internet e alle situazioni di rischio correlate.
- **Garante Regionale per l'Infanzia e l'Adolescenza e Difensore Civico**: segnalano all'Autorità Giudiziaria e ai Servizi Sociali competenti; accolgono le segnalazioni di presunti abusi e forniscono informazioni sulle modalità di tutela e di esercizio dei diritti dei minori vittime. Segnalano alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.
- **Tribunale per i Minorenni**: segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

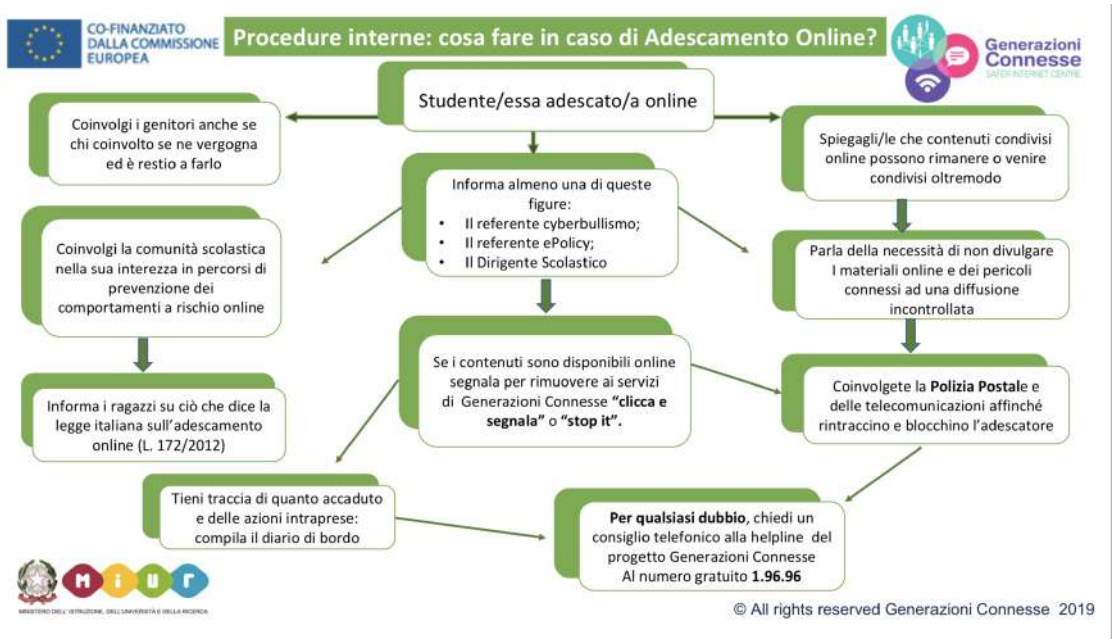
5.4. - Allegati con le procedure

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

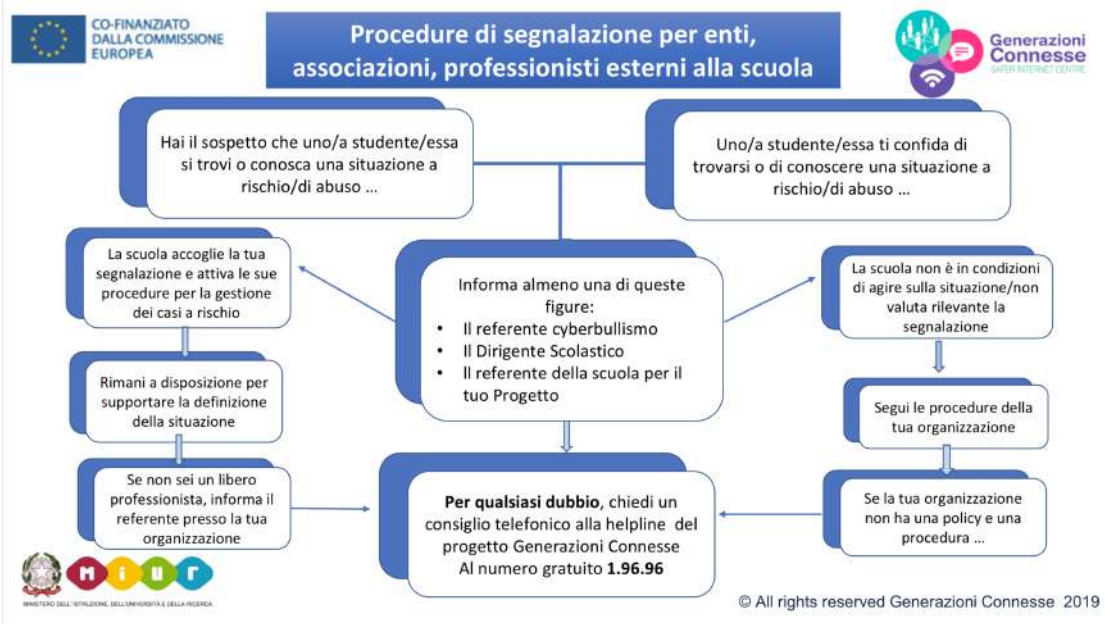
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



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



Altri allegati

- Scheda di segnalazione
- Diario di bordo
- iGloss@ 1.0 l'ABC dei comportamenti devianti online
- Elenco reati procedibili d'ufficio

Il nostro piano d'azioni

Non è prevista nessuna azione.