Istituto d'Istruzione Superiore
Giustino Fortunato – Rionero in Vulture
Liceo Scientifico - Liceo delle Scienze Umane
Liceo Classico - Liceo Artistico

Documento di ePolicy

PZIS002003

I.I.S. "G. FORTUNATO" RIONERO IN V.

S. S. 167 VIA MONTICCHIO CAMPUS - 85028 - RIONERO IN VULTURE - POTENZA

Prof.ssa Antonella Ruggeri

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'Epolicy, inoltre, vuole essere un documento finalizzato a prevenire situazioni problematiche e a riconoscere, gestire, segnalare e monitorare episodi legati ad un utilizzo scorretto degli strumenti.

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

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

Argomenti del Documento

1. **Presentazione dell'ePolicy**
    1. Scopo dell'ePolicy
    2. Ruoli e responsabilità
    3. Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto
    4. Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica
    5. Gestione delle infrazioni alla ePolicy

6. Integrazione dell'ePolicy con regolamenti esistenti
7. Monitoraggio dell'implementazione dell'ePolicy e suo aggiornamento

2. **Formazione e curricolo**
    1. Curricolo sulle competenze digitali per gli studenti
    2. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica
    3. Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali
    4. Sensibilizzazione delle famiglie e Patto di corresponsabilità
3. **Gestione dell'infrastruttura e della strumentazione ICT (Information and Communication Technology) della e nella scuola**
    1. Protezione dei dati personali
    2. Accesso ad Internet
    3. Strumenti di comunicazione online
    4. Strumentazione personale
4. **Rischi on line: conoscere, prevenire e rilevare**
    1. Sensibilizzazione e prevenzione
    2. Cyberbullismo: che cos'è e come prevenirlo
    3. Hate speech: che cos'è e come prevenirlo
    4. Dipendenza da Internet e gioco online
    5. Sexting
    6. Adescamento online
    7. Pedopornografia
    5. **Segnalazione e gestione dei casi**
    1. Cosa segnalare
    2. Come segnalare: quali strumenti e a chi
    3. Gli attori sul territorio per intervenire
    4. Allegati con le procedure

Perché è importante dotarsi di una E-policy?

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

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

1.2 - Ruoli e responsabilità

Affinché l'E-policy sia davvero uno strumento operativo efficace per la scuola e tutta la comunità educante è necessario che ognuno, secondo il proprio ruolo, s'impegni nell'attuazione e promozione di essa.

Il Dirigente Scolastico

Il Dirigente Scolastico è il soggetto su cui incombe la responsabilità di garantire la sicurezza, dei membri della comunità scolastica e, conseguentemente, anche della sicurezza in rete. In quest'ottica si preoccupa di:

- promuovere le buone prassi in linea con il quadro formativi di riferimento e con le indicazioni del M.I., mediante l'organizzazione di percorsi di formazione per la sicurezza e problematiche connesse all'utilizzo della rete sia online che offline, con la collaborazione del docente Referente d'Istituto per le tematiche del Bullismo e del Cyberbullismo;
- coinvolgere, nella prevenzione e contrasto al fenomeno del bullismo, tutte le componenti della comunità scolastica;
- dotare la scuola di un sistema in grado di consentire il controllo della sicurezza in rete;
- favorire la discussione all'interno della scuola, attraverso i vari organi collegiali,per l'uso responsabile e corretto delle Tecnologie dell'Informazione e della Comunicazione, oltre che nell'uso personale, anche nella didattica;
- gestire ed intervenire nei casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali.

L'Animatore digitale

L'Animatore digitale si preoccupa di:

- supportare il personale scolastico da un punto di vista non solo tecnicoinformatico, ma anche in riferimento ai rischi online, alla protezione e gestione dei dati personali;
- promuovere percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale";
- monitorare e rilevare eventuali criticità connesse all'uso delle TIC a scuola proponendo soluzioni adeguate.

Team per l'innovazione digitale

Il Team per l'innovazione digitale ha la funzione di:

- supportare e accompagnare l'innovazione didattica nelle istituzioni scolastiche;
- supportare l'attività dell'Animatore digitale.

Il Referente bullismo e cyberbullismo

Tale figura 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;
- promuovere la conoscenza e la consapevolezza del bullismo e del cyberbullismo attraverso progetti d'istituto che coinvolgano genitori, studenti e tutto il personale;

- coordinare le attività di prevenzione ed informazione sulle sanzioni previste e sulle responsabilità di natura civile e penale anche con eventuale affiancamento di genitori e studenti;
- ricorrere a partner esterni alla scuola, quali servizi sociali e sanitari, aziende del privato sociale, forze di polizia, per realizzare progetti di prevenzione;
- curare i rapporti di rete fra scuole per eventuali convegni/seminari/corsi e per la giornata mondiale sulla Sicurezza in Internet, la "Safer InternetDay".

I Docenti

- informarsi e ad aggiornarsi sul tema della sicurezza in rete uniformandosi alle politiche di sicurezza adottate dalla scuola di cui rispettano il regolamento;
- supportare gli alunni nel corretto utilizzo delle tecnologie digitali per finalità didattico- educative;
- seguire gli studenti nella scelta delle fonti di informazioni;
- garantire che le comunicazioni con i mezzi informatici avvengano nel rispetto delle regole e tramite canali ufficiali e verificabili (posta elettronica con il dominio dell'istituto, GSUITE for Education)
- rispettare l'obbligo di riservatezza dei dati personali trattati e non, in conformità alla normativa vigente;
- seguire le procedure interne di segnalazione di eventuali abusi subiti dagli alunni e connessi all'uso delle tecnologie digitali.

Il DSGA

Il direttore dei servizi generali e amministrativi si preoccupa di:

- assicurare, nei limiti delle risorse finanziarie, la manutenzione delle strutture informatiche al fine del suo funzionamento, della sicurezza e tutela da un uso improprio.

Gli Studenti

Agli studenti è richiesto di:

- utilizzare con responsabilità le tecnologie digitali uniformandosi alle indicazioni dei docenti nonché al rispetto delle norme codificate nei regolamenti di istituto;
- rispettare le buone pratiche di sicurezza in rete;
- saper distinguere, con l'aiuto dei docenti, le fonti di informazione attendibili in rete; • segnalare ai docenti situazioni di difficoltà nell'utilizzo delle tecnologie digitali;

I Genitori

I Genitori, in continuità con la scuola,sono coinvolti nelle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete, nonché sull'uso responsabile dei device personali. Ad essi è richiesto di:

- sostenere i docenti nell'azione educativa diretta al corretto utilizzo delle tecnologie digitale,
- educare(vigilando sui propri figli) al corretto utilizzo delle tecnologie digitali in ambiente domestico fissando regole comportamentali e di utilizzo, in particolare in caso di attività di didattica a distanza;
- collaborare con i docenti nell'adozione di linee di intervento coerenti per contrastare l'uso non responsabile, scorretto o pericoloso delle tecnologiedigitali.

Gli Enti educativi esterni e le associazioni

Agli Enti educativi esterni e alle associazioni che entrano in relazione con la scuola si richiede di:

- conformarsi alla politica della stessa riguardo all'uso consapevole della Rete e delle TIC;
- promuovere comportamenti sicuri, la sicurezza online e la protezione degli studenti 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).

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.

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.

1.6 - Integrazione dell'ePolicy con Regolamenti esistenti

Il Regolamento dell'Istituto Scolastico viene aggiornato con specifici riferimenti all'Epolicy, 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.
Il monitoraggio e la revisione del documento E-policy viene affidato ai docenti Referenti ePolicy coadiuvati dal gruppo di lavoro.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

- Organizzare uno o più eventi o attività volti a presentare il progetto alla comunità scolastica.

Azioni da svolgere nei prossimi 3 anni:

- Organizzare incontri o eventi volti a presentare il progetto agli studenti/studentesse e ai genitori sui temi dell'ePolicy;.
- Organizzare un evento di presentazione del progetto Generazioni Connesse rivolto agli studenti.

Capitolo 2 - Formazione e curricolo

2.1. Curricolo sulle competenze digitali per gli studenti

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

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

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

L'individuazione di aree di competenza e descirttori segue le indicazioni del Dig.com

2.1 - " Il quadro di riferimento per le competenze dei cittadini"

AREE DI COMPETENZA

Area 1: "Alfabetizzazione e dati"

Area 2: "Comunicazione e collaborazione"

Area 3: "Creazione di contenuti digitali"

Area 4: "Sicurezza"

DESCRITTORI DELLE AREE DI COMPETENZA

Area 1

1.1 Navigare, ricercare e filtrare dati, informazioni e contenuti digitali.

1.2 Valutare dati, informazioni e contenuti digitali.

1.3 Gestire dati, informazioni e contenuti digitali.

Area 2

2.1 Interagire attraverso le tecnologie digitali.

2.2 Condividere informazioni attraverso le tecnologie digitali.

2.3 Esercitare la cittadinanza attraverso le tecnologie digitali.

2.4 Collaborare attraverso le tecnologie digitali.

2.5 Conoscere e rispettare la Netiquette.

2.6 Gestire l'identità digitale.

Area 3

3.1 Sviluppare contenuti digitali.

3.2 Integrare e rielaborare contenuti digitali.

3.3 Copyright e licenze.

3.4 Programmazione.

Area 4

4.1 Proteggere i dispositivi.

4.2 Proteggere i dati personali e la privacy.

4.3 Proteggere la salute e il benessere.

4.4 Proteggere l'ambiente.

LIVELLI DI COMPETENZA

Per quanto concerne i livelli di competenza, si rimanda al documento del Dig.com 2.1.

La formazione del curricolo digitale avrà come riferimento l'art. 5 della legge 20 agosto 2019 n. 92 (Introduzione dell'insegnamento scolastico dell'educazione civica) interamente dedicato alla "cittadinanza digitale"

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.

L'IIS Giustuno Fortunato, da tempo, ha avviato un processo volto a favorire l'utilizzo delle tecnologie informatiche nella didattica (registro elettronico, LIM, ambienti di condivisione).

Nelle classi è stato allestito un setting strumentale composto da iPad e personal computer a disposizione degli studenti e dei docenti. I dispositivi sono dotati di molteplici applicazioni digitali, che *in itinere* vengono aggiornate e integrate secondo le esigenze didattiche.

Nell'Istituto sono presenti laboratori informatici di recente implementazione. Tutti i docenti dell'Istituto hanno svolto e continuano a svolgere attività di formazione per un corretto utilizzo dei dispositivi digitali.

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.

Il reading literacy è l'obiettivo che l'Istituto intende raggiungere per consentire a ciascun docenti di raggiungere una assoluta consapevolezza e padronanza delle molteplici opportunità offerte dalle tecnologie digitali legate alla didattica.

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

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

Il nostro piano d'azioni

AZIONI da sviluppare nell'arco dell'anno scolastico 2021/2022

- Prevenzione del bullismo e cyberbullismo.
- Prevenzione dei reati on-line nelle classi quarte.
- Promozione di percorsi formativi per lo sviluppo delle competenze digitali.
- Implementazione della sperimentazione 2.0. Redazione del documento ePolicy.

AZIONI da sviluppare nell'arco dei tre anni scolastici successivi

- Organizzazione di incontri con esperti sulle competenze digitali, sull'educazione alla cittadinanza digitale.
- Coinvolgimento di una rappresentanza di genitori per individuare i temi di maggiore interesse nell'ambito dell'educazione alla cittadinanza digitale.
- Organizzazione e promozione di incontri formativi per il corpo docente sull'utilizzo consapevole e sicuro di Internet e sulle tecnologie digitali.

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

3.1 - Protezione dei dati personali

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

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

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

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

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

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

Il nostro Istituto si è prontamente adeguato alla suindicata normativa adempiendo a quanto in essa prescritto.

Sul sito web dell'Istituto sono state attivate due sezione "Privacy e Altri contenuti" recentemente aggiornate in adempimento al Regolamento PRIVACY 679 del 2016 In questi spazi è possibile consultare:

- tutte le informative aggiornate per il trattamento dati
- la politica di protezione dei dati personali

- nomina DPO
- contatto diretto con il DPO

Inoltre,nella sezione "Aggiornamento organigramma" sono visibili i nominativi di tutto il personale con relativo incarico privacy.

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.
L'istituto è dotato di una strumentazione tecnologica attiva, in modo capillare, in tutti gli spazi. La connettività è garantita da una rete in modalità via cavo e Wi-Fi ed offre la connessione ad internet per le attività sia didattiche sia amministrative. Il Dirigente Scolastico, il corpo docente, il Direttore dei Servizi Generali e Amministrativi, il personale degli uffici della segreteria accedono ai servizi tramite procedura di autenticazione personale che

prevede l'utilizzo di password aventi caratteristiche adeguate. La rete didattica fornisce in sicurezza la connessione alle 44 classi provviste di strumentazione tecnologica, ai laboratori scientifici, multimediali e alle aule multifunzionali.

Gli studenti accedono alla rete sotto il controllo dei docenti e degli assistenti durante le attività didattiche. Gli assistenti tecnici informatici hanno cura di aggiornare periodicamente il software e il sistema operativo a garanzia della protezione da aggressioni esterne.

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.

Relativamente agli ambienti di apprendimento, il nostro Istituto si avvale di:

- n.1 laboratorio di informatica;
- n.2 laboratori multimediali;
- gli studenti e le studentesse possono usufruire di n.319 dispositivi mobili sui quali è possibile scaricare i libri di testo in formato digitale e software di supporto alla didattica

Le comunicazioni verso l'esterno sono affidate ad un sito web, costantemente aggiornato, e ai più comuni social network.

La comunicazione interna avviene tramite:

- il registro elettronico che consente di gestire la comunicazione con le famiglie,
- mail scolastica,
- applicativi e piattaforme che hanno dimostrato tutta la loro affidabilità e utilità in occasione dei periodi di lockdown e di didattica a distanza.

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.

In, particolare, è vietato utilizzare il telefono cellulare e altri dispositivi elettronici e di intrattenimento (tablet, notebook, fotocamera, videocamera, casse, ecc.) durante le attività didattiche in aula e in tutti i locali della scuola, nel rispetto di quanto sancito dal D.P.R. n. 249/1998. Il divieto risponde a una generale norma di correttezza, in quanto l'utilizzo del telefono cellulare o di altri dispositivi elettronici rappresenta un elemento di distrazione sia per chi lo usa sia per il resto della classe. Gli studenti devono tenere i dispositivi spenti e custoditi nei borsoni o zaini.

È consentito ai docenti di organizzare la propria attività didattica mediante utilizzo dei diversi dispositivi elettronici, anche da parte degli studenti, qualora lo si ritenga funzionale all'attività stessa.

Il nostro piano d'azioni

AZIONI da sviluppare nell'arco dell'anno scolastico 2021/2022

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

AZIONI da sviluppare nell'arco dei tre anni scolastici successivi

- 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 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) .
- Organizzazione di incontri con esperti sulle competenze digitali, sull'educazione alla cittadinanza digitale.
- Coinvolgimento di una rappresentanza di genitori per individuare i temi di maggiore interesse nell'ambito dell'educazione alla cittadinanza digitale.
- Organizzazione e promozione di incontri formativi per il corpo docente sull'utilizzo consapevole e sicuro di Internet e sulle tecnologie digitali.

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.*

Le fasi attuative dal punto di vista operativo si possono declinare come segue:

1. Programmare degli interventi mirati, con l'ausilio di eventuali esperti esterni in materia, dove si analizzano determinate problematiche o condizioni;
2. Raccogliere il feedback da parte degli studenti.

Nel caso della **prevenzione** si distinguono tre tipi di prevenzione:

1) Quella universale presuppone che tutti gli studenti siano potenzialmente a rischio,quindi si rivolge ad un grande pubblico;
2) Quella selettiva che si rivolge ad un gruppo scelto in base a precedenti indagini e segnalazioni;
3) Quella indicata che consiste in un intervento su caso specifico.

In questo ultimo caso risulta opportuno coinvolgere anche la famiglia.

L'istituto metterà a disposizione una scheda di segnalazione accessibile al personale docente e un modulo/mail per gli studenti al fine di permettere loro di segnalare/denunciare, in piena riservatezza, una situazione di bisogno.

L'istituto favorisce la raccolta ed utilizzo di materiale esplicativo uniformato e condiviso per agevolare e armonizzare le azioni di 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** prevenzione **del Referente per le iniziative di prevenzione e contrasto che:**
    - Ha il compito di coordinare le iniziative di 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).

Il nostro istituto ha istituito il team anti bullismo, anti cyberbullismo e per l'emergenza le cui linee programmate sono:

- Promozione di iniziative di carattere culturale, sociale e sportivo sui temi del rispetto delle diversità, dell'educazione alla legalità e all'uso consapevole della rete internet.
- Organizzazione di corsi di formazione per il personale scolastico volti a far acquisire tecniche e pratiche educative efficaci nella prevenzione del fenomeno del bullismo con particolare attenzione ai rischi

provenienti dai modelli culturali potenzialmente lesivi della dignità della persona, veicolati dai mezzi di comunicazione e dal web.

- Organizzazione di corsi e programmi di assistenza volti a far acquisire ai genitori la consapevolezza del fenomeno e delle sue manifestazioni, la capacità di decodificarne i segnali, nonché l'importanza del dialogo con i figli - vittime di soprusi o spettatori di violenze o con coloro che si sono resi responsabili di azioni di bullismo.
- Attivazione di percorsi di sostegno in favore dei minori vittime, autori e spettatori di atti di bullismo, dei gruppi classe in cui si è verificato l'evento, nonché di sportello di ascolto o, con il supporto di competente figura professionale, per stimolare la consapevolezza degli schemi comportamentali disfunzionali che bullo, vittima e spettatori attivano.

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.

Azioni:

- potenziamento delle competenze sociali e civiche;
- promozione negli studenti di comportamenti empatici e pro sociali;
- promozione negli studenti di buone prassi comportamentali;
- promozione della sicurezza in Rete degli studenti, perché acquisiscano le competenze necessarie all'esercizio di una cittadinanza digitale consapevole;
- realizzazione di un'alfabetizzazione emotiva, individuando nell'analfabetismo emotivo, accresciuto dai mezzi tecnologici, la causa prima di atteggiamenti sociali violenti e intenzionali, di natura sia fisica che psicologica;
- promozione della costruzione di un ambiente emotivamente sano, perché esso costituisce un terreno fertile per l'apprendimento e la socializzazione.

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?

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

- presenza di referenti su bullismo e cyberbullismo;
- attività di Sportello di ascolto;
- collaborazione con la ASL per l'educazione alla sessualità e all'affettività;
- incontri con la Polizia Postale;
- progetti di attività didattica mirati all'accettazione dell'altro e all'inclusione.

L'Istituto adotta, all'interno del proprio curricolo per l'educazione civica, tutti gli strumenti necessari per riconoscere e prevenire la dipendenza da internet e dal gioco online, attraverso la realizzazione di una serie di unità didattiche e attività legate alla sensibilizzazione su questo tema.

4.5 - Sexting

Il "sexting" è fra i rischi più diffusi connessi ad un uso poco consapevole della Rete. Il termine indica un fenomeno molto frequente fra i giovanissimi che consiste nello scambio di contenuti mediali sessualmente espliciti; i/le ragazzi/e lo fanno senza essere realmente consapevoli di scambiare materiale (pedopornografico) che potrebbe arrivare in mani sbagliate e avere conseguenze impattanti emotivamente per i protagonisti delle immagini, delle foto e dei video.

Il "Giustino Fortunato" in relazione a questa problematica programmerà:

- partecipazione ad eventi e incontri della Polizia Postale;
- cicli di incontri con l'Arma dei Carabinieri per la prevenzione e la sensibilizzazione sui reati legati all'utilizzo di internet e delle piattaforme online;
- presenza a scuola di referenti bullismo e cyberbullismo;
- presenza a scuola del referente dello Sportello d'ascolto.

L'Istituto adotta, inoltre, all'interno del proprio curricolo per l'educazione civica, tutti gli accorgimenti per riconoscere e prevenire il fenomeno del sexting, anche attraverso la realizzazione di unità didattiche e attività legate alla sensibilizzazione su questo 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.

Il G. Fortunato promuove azioni di sensibilizzazione e prevenzione anche relativamente a questo argomento, in modo particolare organizzerà una serie di iniziative volte a:

- Far conoscere e riconoscere ai ragazzi i pericoli della Rete: pedofilia e cyber bullismo.
- Istruire i ragazzi in merito alle strategie comportamentali per ridurre i rischi di esposizione.
- Attuare interventi di educazione all'affettività.
- Promuovere interventi di collaborazione, tutoring aiuto reciproco.
- Attuare percorsi di educazione alla convivenza civile e alla cittadinanza.

Il curricolo per l'educazione civica prevede l'attuazione di strumenti necessari per riconoscere e prevenire l'adescamento online, attraverso unità didattiche e attività legate alla sensibilizzazione su questo tema volte a rendere gli studeniti più consapevoli e critici nei confronti dei loro rapporti online. A riguardo, è fondamentale per l'Istituto la collaborazione con la psicologa della scuola.

4.7 - Pedopornografia

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

La legge n. 269 del 3 agosto 1998 *"Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di schiavitù", introduce nuove fattispecie di reato (come ad esempio il turismo sessuale) e, insieme alle successive modifiche e integrazioni contenute nella* ***legge n. 38 del 6 febbraio 2006*** *"Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet"*, segna una tappa fondamentale nella definizione e predisposizione di strumenti utili a contrastare i fenomeni di sfruttamento sessuale a danno di minori. Quest'ultima, introduce, tra le altre cose, il reato di "pornografia minorile virtuale" (artt. 600 ter e 600 quater c.p.) che si verifica quando il materiale

pedopornografico rappresenta immagini relative a bambini/e ed adolescenti, realizzate con tecniche di elaborazione grafica non associate, in tutto o in parte, a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali.

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

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

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

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

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

In un'ottica di attività preventive il nostro Istituto programmerà frequenti incontro la Polizia Postale per tutti gli alunni al fine di far conoscere gli strumenti di comunicazione/interazione in Internet, i possibili rischi, l'esistenza e l'utilizzo di sistemi di controllo per la configurazione personalizzata dei computer della scuola e di casa.

COMPETENZE

- Utilizzare netiquette e norme di uso corretto dei servizi di Rete.
- Saper applicare le regole di scrittura per le e-mail.
- Utilizzare i nuovi strumenti per tutelare la privacy, volti a garantire alle persone maggiore trasparenza e controllo sulle informazioni che condividono sui social network e decalogo della privacy digitale.
- Acquisire la consapevolezza dell'importanza del rispetto delle regole, dei canoni comportamentali da assumere nella comunità sociale e delle norme giuridiche che regolano gli stessi.
- Riconoscere " i pericoli nascosti" negli strumenti di comunicazione/interazione attualmente disponibili su internet quali i social network (Facebook, Myspace), le chat e l'instantmessaging (Twitter, Whatsapp), la pubblicazione di contenuti (Youtube).

Il nostro piano d'azioni

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

- 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 e ai docenti, con il coinvolgimento di esperti.
- Organizzare uno o più incontri di formazione all'utilizzo sicuro e consapevole di Internet e delle tecnologie digitali integrando losvolgimento 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 laboratori di educazione alla sessualità e all'affettività, rivolti agli/lle studenti/studentesse.
- Organizzare uno o più eventi e/o dibattiti in momenti extrascolastici, 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.

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.
- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti agli/lle studenti/studentesse, con il coinvolgimento di esperti.
- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti.
- Organizzare uno o più incontri 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 laboratori di educazione alla sessualità e all'affettività, rivolti agli/lle studenti/studentesse.
- Organizzare uno o più eventi e/o dibattiti in momenti extrascolastici, 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.

Si considerano da segnalare tutte quelle situazioni caratterizzate da volontarie e ripetute aggressioni che mirano a insultare, minacciare, diffamare e/o ferire una persona (o un piccolo gruppo) tramite un utilizzo irresponsabile delle TIC.

In particolare si segnaleranno:

- contenuti che violano la privacy;
- contenuti aggressivi o violenti;
- contenuti di natura sessuale.

Tutte le segnalazioni riportate dai docenti verranno registrate su apposita scheda.

5.2. - Come segnalare: quali strumenti e a chi

L'insegnante riveste la qualifica di pubblico ufficiale in quanto l'esercizio delle sue funzioni non è circoscritto all'ambito dell'apprendimento, ossia alla sola preparazione e tenuta delle lezioni, alla verifica/valutazione dei contenuti appresi dagli studenti e dalle studentesse, ma si estende a tutte le altre attività educative.
Le situazioni problematiche in relazione all'uso delle tecnologie digitali dovrebbero essere sempre gestite anche a livello di gruppo.
Come descritto nelle procedure di questa sezione, si potrebbero palesare due casi:

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

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

Strumenti a disposizione di studenti/esse

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

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

Anche studenti e studentesse, inoltre, possono rivolgersi alla Helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.
Le segnalazioni potranno essere inviate al:

- **Dirigente Scolastico** antonella.ruggeri@liceirionero.edu.it
- **Referente del Cybrbullismo** antonella.gamma@liceirionero.edu.it
- **Funzione Strumentale** rosa.stia@liceirionero.edu.it
- **Animatrice Digitale** raffaella.mosca@liceirionero.edu.it

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

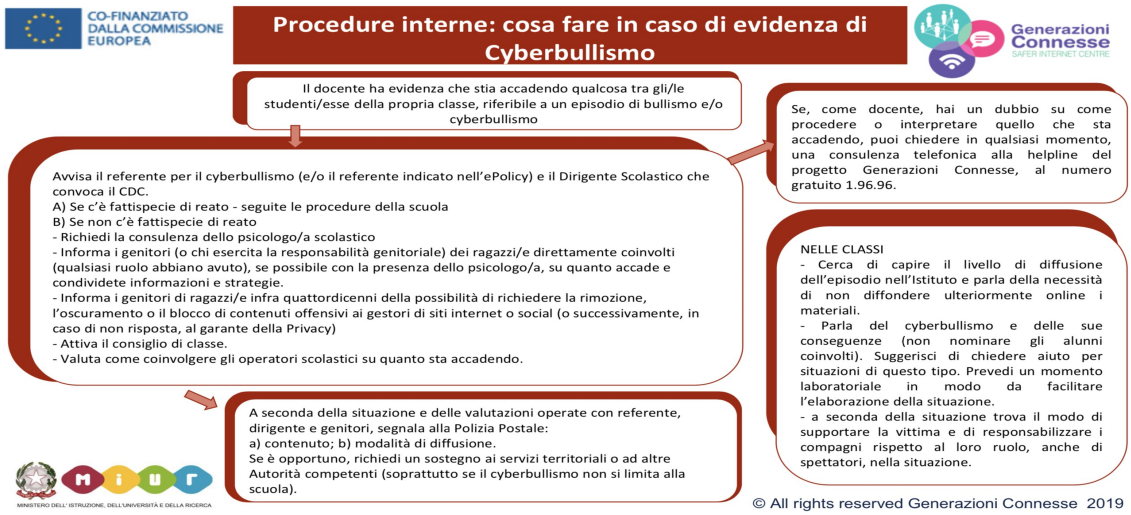
tecnologie digitali da parte dei più giovani" (seconda parte, pag. 31), senza dimenticare che la Helpline di Telefono Azzurro (19696) è sempre attiva nell'offrire una guida competente ed un supporto in tale percorso.
A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all'utilizzo di Internet può presentare.

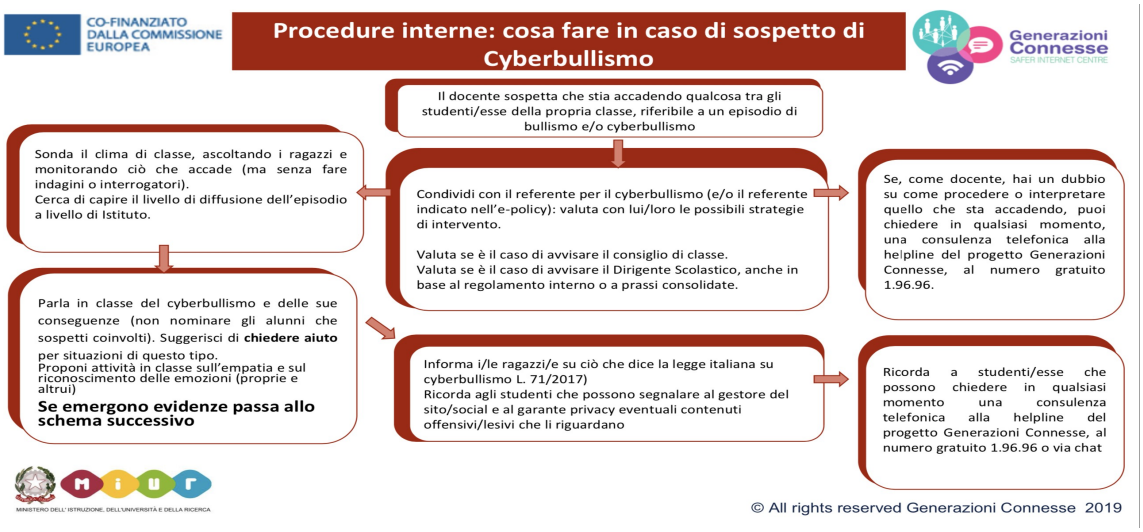
- **Comitato Regionale Unicef**: laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni)**: svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare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

- **Comitato** Regionale Unicef: comitato.basilicata@unicef.it
  Tel: 0971 472042
  Fax: 0971 1780219
- Co.Re.Com Basilicata: corecom@regione.basilicata.it
  Tel: 0971447055 - 447088 - 447063
- Ufficio scolastico regionale: Regione Basilicata direzionebasilicata@istruzione.it
  Tel. 0971/ 449911
- Polizia postale e delle comunicazioni: compartimento.polposta.pz@pecps.poliziadistato.it
  Tel. 0971 327364
- Garante Regionale per l'Infanzia e l'Adolescenza e Difensore Civico:
  garanteinfanziaeadolescenza@regione.basilicata.it
  garanteinfanziaeadolescenza@pec.consiglio.basilicata.it

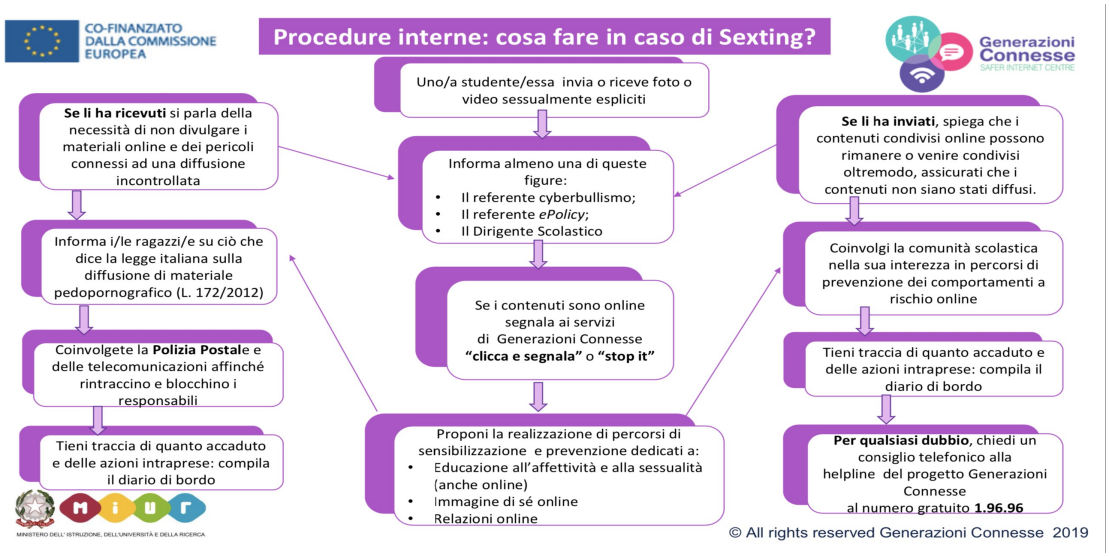
5.4. - Allegati con le procedure

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

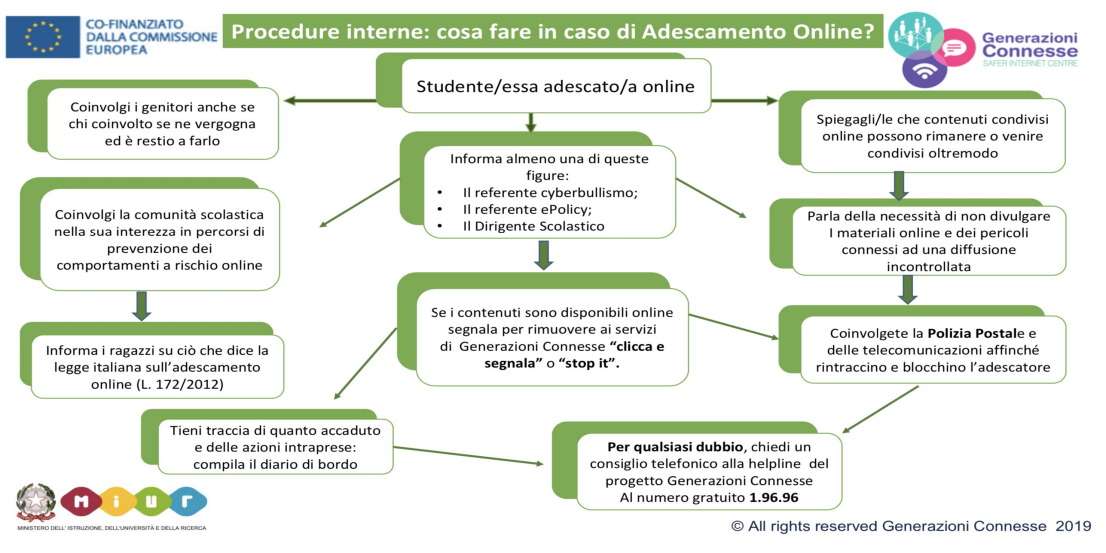




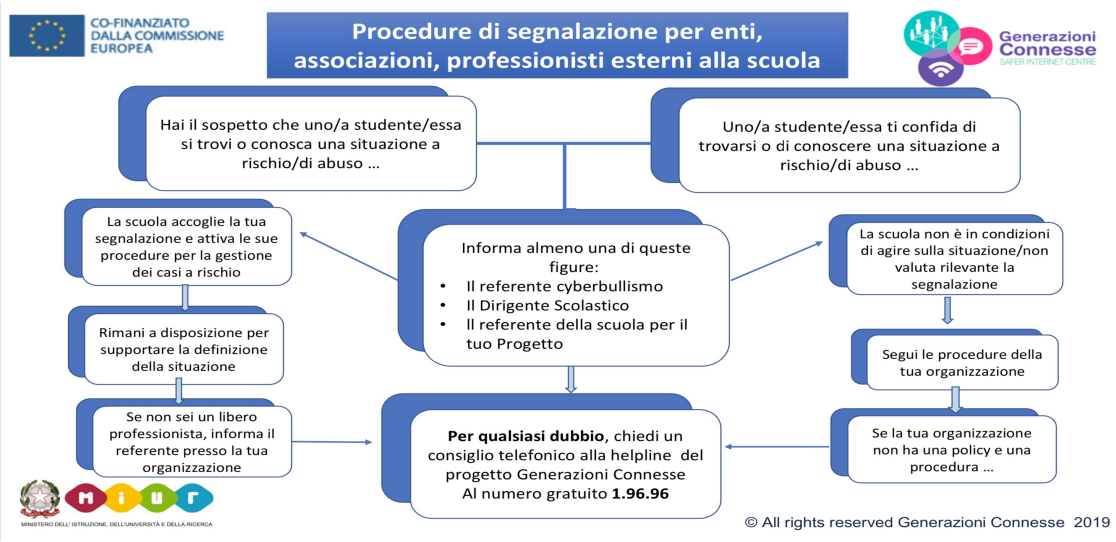
Procedure interne: cosa fare in caso di sexting?



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

Sulla base delle Linee Guida per l'uso positivo delle tecnologie digitali e della prevenzione dei rischi nelle scuole, vengono assunti i seguenti punti quali indicatori di co-costruzione tra scuola-famiglia-servizi territoriali, al fine di creare un modello composito e lineare di azioni condivise:

- coinvolgimento di tutti gli attori della scuola: studenti e studentesse, docenti, genitori e personale ATA, per la realizzazione di una autentica comunità educante;
- alleanza educativa tra scuola e famiglia interventi educativi ed azioni di supporto, quale prevenzione per eventuali comportamenti a rischio;
- misure preventive specifiche di tutela anche con l'ausilio di attori territoriali, come forze dell'ordine ed ASP per servizi specialistici;
- promozione dell'educazione al rispetto;
- sviluppo del pensiero critico;
- promozione dell'Educazione Civica Digitale;
- monitoraggio dei fenomeni di bullismo e cyberbullismo per studenti e docenti attraverso questionari - Piattaforma Elisa.

Firmato digitalmente da

ANTONELLA RUGGERI

CN = RUGGERI ANTONELLA
C = IT