Documento di ePolicy

PDIC853006

IC CARRARESE EUGANEO

VIA ROMA69 - 35020 - DUE CARRARE - PADOVA (PD)

Burattin Matteo

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

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.

Questo documento può essere aggiornato in futuro con l'ampiamento delle TIC a disposizione dell'Istituto e al sopraggiungere di nuove esigenze.

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

è garante della sicurezza, anche online, di tutti i membri della comunità scolastica; promuove la cultura e la sicurezza, anche affiancando il referente bullismo/cyberbullismo e l'animatore digitale nell'organizzazione di eventi formativi per un utilizzo positivo e responsabile delle TIC; interviene e gestisce i casi gravi di uso improprio delle TIC, bullismo e cyberbullismo; supervisiona affinché le corrette modalità di utilizzo sicuro delle TIC siano integrate nei regolamenti scolastici e nelle attività didattiche e educative.

L'animatore digitale

promuove e organizza la formazione nei suoi ambiti di competenza; rileva e monitora le problematiche relative all'utilizzo delle TIC e di internet a scuola; supporta l'intero personale non solo per la gestione tecnologica, ma anche per la gestione e la protezione dei dati e i rischi online; assiste gli utenti autorizzati nella gestione dell'account fornito dall'Istituto, secondo gli usi consentiti.

Il referente bullismo e cyberbullismo

in collaborazione con il dirigente scolastico coordina e promuove iniziative per il contrasto al bullismo e al cyberbullismo; promuove la formazione della

comunità scolastica; raccoglie le segnalazioni di bullismo e cyberbullismo seguento le procedure previste dall'Istituto; collabora con le forze di Polizia e con le associazioni del territorio.

I docenti

si formano nei campi attinenti la gestione della tecnologia, delle risorse digitali e di internet, nonché sulla gestione dei dati e la sicurezza; diffondono la cultura dell'uso responsabile delle TIC e della rete; integrano, laddove possibile, l'utilizzo delle tecnologie digitali nei propri percorsi didattici; hanno il dovere morale e professionale di segnalare al dirigente qualsiasi abuso o violazione, anche online, che veda coinvolti gli studenti e le studentesse, per l'adozione delle misure previste dalle norme.

Il personale amministrativo, tecnico e ausiliario, ATA

è coinvolto nella formazione contro il bullismo e il cyberbullismo; può essere coinvolto nella segnalazione di comportamenti non adeguati al regolamento scolastico e/o di bullismo e cyberbullismo e nel raccogliere, verificare e valutare informazioni importanti per l'emergere degli stessi.

Le studentesse e gli studenti

sono portati, in relazione al proprio grado di maturità e di apprendimento, ad acquisire le proprie responsabilità nell'utilizzo dei sistemi delle tecnologie digitali, guidati dalle famiglie e dai docenti; sono invitati a comprendere le potenzialità e i rischi delle attività online; adottano condotte rispettose nella comunicazione; sono invitati a esprimere domande o bisogni relativi all'utilizzo delle tecnologie e di internet ai docenti e alle famiglie.

I genitori

partecipano attivamente all'educazione ad un uso consapevole e responsabile delle TIC e dei device personali; si relazionano costruttivamente con i docenti e il personale interessato per intervenire in caso di situazioni di rischio o di eventuali problemi nella gestione delle tecnologie e in generale sulle linee educative adottate; sottoscrivendo il patto di corresponsabilità si impegnano ad accettare e condividere quanto riportato nel documento epolicy di Istituto.

Gli enti educativi esterni e le associazioni

se entrano in relazione con l'Istituto devono conformarsi alla sua politica riguardo l'uso delle TIC e della rete, promuovono la sicurezza online e vigilano affinché essa venga mantenuta durante le attività che li vedono coinvolti

---

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).

Le figure professionali esterne e le organizzazioni, gli esperti a vario titolo coinvolti in progetti, laboratori e attività di breve o lungo periodo, sono tenuti a prendere visione dei documenti e dei regolamenti proposti dall'Istituto e sottoscriverli preliminarmente all'avvio delle attività stesse.

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.

Verranno proposte delle sintesi adatte al livello di maturità e di apprendimento del documento di e policy per gli studenti e le studentesse; sarà incoraggiato nelle famiglie un atteggiamento di collaborazione nel perseguimento della sicurezza online e nell'uso delle tecnologie anche in occasione delle assemblee e riunioni previste dall'organizzazione scolastica; saranno promosse tra i docenti e il personale attraverso materiale informativo le buone pratiche elencate nell'epolicy.

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.

Le infrazioni all'epolicy verranno gestite dalla scuola attraverso azioni educative e, qualora fossero necessarie, sanzioni, valutando volta per volta i

diversi gradi di gravità delle violazioni.

A seconda dell'età degli studenti e delle studentesse saranno proposte diverse attività educative e di sensibilizzazione, valutando anche il coinvolgimento di tutto il gruppo classe.

Per eventuali sanzioni, rapportate all'età degli studenti e alla gravità dei fatti, si fa riferimento al regolamento d'Istituto.

Possono essere previsti interventi di carattere educativo, volti ad una chiara e condivisa definizione delle regole sociali di convivenza e alla gestione di problematiche emerse.

Più avanti in questo documento saranno elencati i principali rischi online e violazioni a cui porre particolare attenzione.

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.

Si integrano il Ptof, il regolamento d'Istituto, il regolamento d'uso della piattaforma Workspace, il patto di corresponsabilità, la netiquette e lo Statuto delle studentesse e degli studenti.

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 l'aggiornamento dell'epolicy, su mandato e sorveglianza degli organi collegiali e su coordinamento del dirigente scolastico, saranno curati dal team per l'epolicy e la prevenzione al bullismo e cyberbullismo e dagli animatori digitali. Esso parte dall'analisi della situazione all'inizio e alla fine dell'anno scolastico, riguardo l'uso consapevole e responsabile delle tecnologie digitali e della rete.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

- Organizzare almeno un evento di presentazione del progetto Generazioni Connesse rivolto agli studenti
- Organizzare almeno un evento di presentazione del progetto Generazioni Connesse rivolto ai docenti
- Organizzare almeno un evento di presentazione del progetto Generazioni Connesse rivolto ai genitori

Azioni da svolgere nei prossimi 3 anni:

- Organizzare almeno un evento di presentazione e conoscenza dell'ePolicy rivolto agli studenti
- Organizzare almeno un evento di presentazione e conoscenza dell'ePolicy rivolto ai docenti
- Organizzare almeno un evento di presentazione e conoscenza dell'ePolicy rivolto ai genitori

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'istituto sostiene il processo di implementazione delle competenze digitali con un curricolo trasversale, per competenze, interdisciplinare. Per sostenere tale processo organizza iniziative formative sulla didattica per competenze e sull'uso delle TIC.

Tenendo conto del Piano Scuola Digitale (PNSD) si pone particolare riguardo allo sviluppo del pensiero computazionale e all'utilizzo critico e consapevole della rete e ai legami con il mondo del lavoro.

L'Istituto punta alla creazione di ambienti didattici finalizzati a creare spazi di apprendimento innovativi. Lo scopo è quello di promuovere lo sviluppo delle abilità cognitive, emotive e relazionali, in accordo con le linee pedagogiche previste.

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.

Con l'ausilio degli animatori digitali vengono organizzati periodicamente corsi di aggiornamento e formazione interni per l'utilizzo delle TIC. Vengono pertanto definiti momenti specifici, soprattutto all'inizio dell'anno scolastico, per uniformare queste competenze e diffondere le buone pratiche. Viene altresì stimolata la segnalazione di eventuali problematiche, in ottica di miglioramento e progressione.

Vengono poi promossi corsi di formazione esterni, proposti dalla Rete o scelti liberamente dai docenti, per lo sviluppo della didattica per competenze, per l'utilizzo sicuro e consapevole delle Tecnologie, anche in ottica di coinvolgimento, inclusione e partecipazione degli alunni.

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.

Nell'Istituto è attiva la figura del referente per le attività di contrasto e prevenzione al bullismo e cyberbullismo (L: 71/2017). La formazione ad un uso sicuro e consapevole delle TIC è estesa anche ad altre figure del team antibullismo.

Si rende comunque necessaria la formazione di tutto il personale docente sull'uso consapevole e sicuro di internet e sui rischi della rete e del trattamento di dati.

La scuola promuove iniziative mediante corsi di aggiornamento, conferenze, seminari interni ed esterni e qualsiasi altra iniziativa promuova un uso sicuro e consapevole delle TIC.

Ci si avvale in particolare, su indicazione dell'Ufficio Scolastico Regionale delle piattaforme "Generazioni connesse" e "Elisa" per il corso "Bullismo e cyberbullismo: conoscenza, valutazione e indicazioni per la prevenzione".

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.

Attraverso il "Patto di corresponsabilità", condiviso e sottoscritto all'inizio dell'anno scolastico, scuola e famiglia si inseriscono in un percorso di dialogo, collaborazione, impegno e rispetto reciproco.

Sul sito scolastico sono presenti i regolamenti e la netiquette e le buone

pratiche vengono divulgate anche con l'assegnazione dell'account personale d'Istituto.

In questo modo la comunità educante è allineata e le figure prese in causa possono portare il proprio contributo al miglior sviluppo delle studentesse e degli studenti, compresa la condivisione di intenti e regole in ambienti digitali.

Sono previsti incontri formativi e informativi sui possibili rischi della rete e per la diffusione dell'epolicy, avvalendosi anche della collaborazione con la Polizia postale.

Viene diffuso il materiale informativo della piattaforma "Generazioni connesse" e di altri siti tematici.

Il nostro piano d'azioni

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

- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.

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.

Sul sito della scuola è consultabile una sezione dedicata alla privacy in cui vengono fornite tutte le informazioni in materia di gestione dei dati personali del nostro Istituto.

Il materiale è consultabile al seguente link:

https://iccarrareseeuganeo.edu.it/privacy-link/

3.2 - Accesso ad Internet

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

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

Il diritto di accesso a Internet è dunque presente nell'ordinamento italiano ed europeo e la scuola dovrebbe essere il luogo dove tale diritto è garantito, anche per quegli

studenti che non dispongono della Rete a casa. In modo coerente il PNSD (Piano Nazionale Scuola Digitale) ha tra gli obiettivi quello di “fornire a tutte le scuole le condizioni per l’accesso alla società dell’informazione e fare in modo che il “diritto a Internet” diventi una realtà, a partire dalla scuola”.

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

Il diritto ad internet è garantito dalla scuola tramite un'infrastruttura di rete adeguata al numero di utenti e in grado di sopportare il traffico generato dalla varie attività che vi si svolgono.

La connssione è in fibra, cablata e wifi, e dotata di firewall.

L'accesso alla rete internet della scuola è gestito dall'Amministratore di sistema. L'accesso alla rete internet è consentito per la didattica in tutti i plessi della scuola: Scuola dell'Infanzia, Scuole Primarie e Scuole Secondarie di Primo Grado. L'accesso avviene tramite reti wifi, protette da password.

Interventi periodici di manutenzione vengono programmati o eseguiti in seguito a segnalazioni specifiche.

I computer dei laboratori informatici e ad uso dei docenti e degli alunni e le LIM hanno impostazioni definite dai responsabili degli stessi e dall'Amministratore di sistema, che si occupano anche di segnalare tempestivamente necessità e problematiche, malfunzionamenti o disservizi.

L'accesso a tali strumenti da parte degli studenti avviene sempre in presenza dell'insegnante di riferimento.

Vengono fornite credenziali personali per l'accesso ai vari portali di interazione con l'Istituzione scolastica (Segreteria digitale, PON, Istanze online, Registro elettronico, ecc.)

Il personale docente e ATA e gli alunni, nonché il Dirigente Scolastico vengono associati ad un account personale con il dominio "@iccarrareseeuganeo.edu.it" con il quale si ha accesso alla Gsuite per estendere le potenzialità della didattica e per gestire la posta elettronica.

Regolamenti e buone pratiche di utilizzo vengono diffuse ai docenti, agli studenti e a tutti gli utenti nelle fasi formative e comunque ogni volta che se ne riscontra la necessità.

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 si avvale per la gestione della comunicazione online e la rappresentanza del sito web raggiungibile all'indirizzo:

https://iccarrareseeuganeo.edu.it/

Il sito web rappresenta lo strumento principale della scuola di comunicazione ufficiale verso l'esterno, promuovendo le attività e guidando l'utenza interessata attraverso i vari modi di interagire con essa.

La gestione del sito (anche per quanto concerne accuratezza, appropriatezza e aggiornamento) e la rispondenza alle norme sono a cura del dirigente scolastico e dei docenti referenti.

Sul sito è possibile accedere agli eventi, le comunicazioni, gli avvisi, la documentazione, la modulistica, link a siti di interesse come al sito del Ministero dell'Istruzione e al registro elettronico.

Il sito si struttura in diverse sezioni dedicate alla scuola, i servizi, le comunicazioni e la didattica.

Sempre tenendo conto della tutela della privacy, la scuola pubblica sul sito i contenuti che vengono giudicati pertinenti alle finalità educative e istituzionali.

Inoltre nell'Istituto viene adottata la piattaforma di lavoro online "Google workspace, Google Suite for education", una piattaforma integrata a marchio Google che consente di comunicare e di gestire contenuti digitali funzionali alle attività didattiche.

Le app della piattaforma vengono verificate per quanto concerne la loro sicurezza in termini di privacy e connessione tra docenti e studenti.

Studenti e docenti hanno accesso ad una serie di servizi, tra cui ci sono per esempio:

- Email personale e spazio di archiviazione afferente

-Drive per produzione e gestione di vari tipi di file: documenti, presentazioni, moduli, fogli di lavoro

-Classroom, che mette a disposizione aule virtuali, servizi di comunicazione, scambio di materiali aggiuntivi.

Si ricorda ai genitori che i servizi a disposizione degli alunni, dopo aver firmato apposita informativa, sono ad uso ESCLUSIVAMENTE SCOLASTICO E DIDATTICO.

Nel momento in cui gli account degli studenti vengono attivati i genitori sono responsabili della vigilanza sull'utilizzo degli stessi al difuori della scuola, e sui dispositivi personali, in particolare sulle finalità esclusavamente didattiche in accordo con i docenti. E' vietato l'utilizzo dell'accounto scolastico per l'adesione a piattaforme non autorizzate.

Strumento principale di comunicazione interna tra scuola e famiglia è il Registro elettronico, che permette di gestire la visualizzazione di informazioni essenziali:

assenze, argomento delle lezioni e compiti, note disciplinari, risultati scolastici, colloqui con gli insegnanti, annotazioni e informazioni varie.

I dispositivi tecnologici della scuola sono programmati per effettuare aggiornamenti periodici del software e per la cancellazione dei cookies in modo da limitare gli errori durante la gestione degli account personali. Ognuno è tenuto a gestire con massima cura i dati personali contenuti nella documentazione e farne un uso strettamente limitato ai loro ambiti di necessità.

In riferimento all'uso di strumenti di comunicazione online è importante ricordare il "diritto alla disconnessione" come da CCNL "Istruzione e Ricerca", 2016-2018, art. 22 comma 4, al fine di conciliare vita lavorativa e vita familiare e personale.

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.

E' fatto divieto di usare il cellulare e altri dispositivi personali come tablet e simili.

Come indicato nel regolamento d'Istituto

https://iccarrareseeuganeo.edu.it/documento/regolamento-di-istituto/

l'uso di questi dispositivi è proibito e in caso di violazione delle norme si rimanda alle indicazioni nel documento indicato.

Il nostro piano d'azioni

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

- 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 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 incontri per la consultazione dei genitori su

indicazioni/regolamenti sull'uso dei dispositivi digitali 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 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.*

Nel nostro Istituto è stato nominato un referente per le azioni contro il bullismo e il cyberbullismo per l'a.s. 2022/2023 e 2023/24:

prof. Andrea Fincato, che ha il compito di:

diffondere la conoscenza dei fenomeni del bullismo e del cyberbullismo nella comunità scolastica attraverso progetti d'Istituto;

coordinare le azioni di azione e prevenzione sui fenomeni, nonché la conoscenza delle responsabilità civili e penali;

collaborare con agenti esterni all'Istituto per organizzare progetti di prevenzione e sensibilizzazione contro bullismo e cyberbullismo;

accogliere e monitorare eventuali segnalazioni di bullismo e cyberbullismo;

coordinare il "team Antibullismo" e il "team per le emergenze".

Secondo le linee di orientamento il "team Antibullismo è formato dal Dirigente Scolastico, il referente antibullismo e cyberbullismo, l'animatore digitale, la psicologa d'Istituto, la referente per l'inclusione e altro personale che permette il miglior coinvolgimento dei vari plessi. Esso collabora per la redazione del presente documento di epolicy e organizza e promuove le varie attività di formazione, sensibilizzazione e prevenzione.

Il "Team per le emergenze" è costituito dagli stessi membri del "team Antibullismo" a cui si aggiungono eventuali professionalità specifiche che possono intervenire in caso di emergenza o casi particolari. Esso valuta e gestisce eventuali casi di bullismo e cyberbullismo e coordina le diverse tipologie di intervento.

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).

Il cyberbullismo si distingue dal bullismo per alcune peculiarità:

gli atti di cyberbullismo possono avvenire "in qualsiasi luogo e in qualsiasi momento", nel senso che attraverso la rete la comunicazione può avvenire in qualsiasi momento del giorno e della notte e essere effettuata da qualsiasi luogo. Inoltre un'offesa, un insulto, un'immagine, un video possono essere condivisi con un numero potenzialmente elevatissimo di persone;

I testimoni possono essere tantissimi;

Il cyberbullo può essere sconosciuto alla vittima, o rimanere più facilmente nell'anonimato;

Il cyberbullo non vede la conseguenza delle sue azioni, ciò limita ulteriormente lo sviluppo di empatia nei confronti della vittima. Ciò vale per il bullo, ma anche per i testimoni compiacenti;

l'utilizzo di identità fittizie può contribuire ulteriormente a processi di deresponsabilizzazione.

Il nostro istituto partecipa ogni anno al "Safer Internet Day" promosso da "Generazioni Connesse", evento online rivolto agli studenti per la sensibilizzazione e la prevenzione di atti di bullismo e cyberbullismo.

Vengono organizzati incontri con la Polizia Postale per chiarire a studenti e docenti eventuali rischi e sanzioni, le attività illecite e le loro conseguenze.

Vengono diffuse proposte di formazione sul tema organizzate dalla Rete di scuole o da Enti del territorio, rivolte a docenti e genitori.

Si ricorda che le azioni di bullismo e cyberbullismo possono includere comportamenti penalmente rilevanti, secondo il Codice Italiano come:

percosse (art. 581)

lesioni personali (art. 582)

ingiuria (art. 594)

diffamazione (art. 595)

violenza privata (art. 610)

minaccia (art. 612)

atti persecutori (art. 612 bis)

danni alle cose, danneggiamento (art. 635)

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.

L'istituto intende promuovere lo sviluppo di competenze digitali e soprattutto l'educazione all'uso etico e consapevole della rete, riconoscendo il ruolo centrale che esse assumono, anche al fine di promuovere nei ragazzi la comprensione di dinamiche rischiose e di incitamento all'odio.

E' fondamentale saper riconoscere l'Hate speech", nella sua complessità e nelle sue caratteristiche, partendo dagli stereotipi che lo alimentano e considerando il suo impatto sulla vita delle persone.

In particolare si promuove la formazione e l'autoformazione da parte di docenti, famiglie e alunni, anche attraverso il materiale qui di seguito afferente alla piattaforma "Generazioni connesse".

il libro diffuso dal Consiglio europeo: "No Hate speech. Idee contro il discorso d'odio attraverso l'educazione ai diritti umani"

https://www.generazioniconnesse.it/_file/documenti/No_HATE/NO%20HATE_ITA_DEF.pdf

La serie di video animati "I Super errori", che parla dei vari rischi della rete con un target specifico per gli alunni degli ultimi anni delle scuole Primarie e quelli delle scuole Secondarie di Primo grado

https://www.generazioniconnesse.it/site/it/0000/00/00/x-la-miniserie-x/

L'istituto si può avvalere per le attività formative di esperti esterni (formazione territoriale, Polizia Postale, associazioni preposte) e/o della psicologa d'Istituto.

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 si propone di fornire agli studenti, ai docenti e alle famiglie strumenti finalizzati al riconoscimento e alla prevenzione del fenomeno.

Formare e formarsi per ricercare il "benessere digitale" significa avere una relazione sana con la tecnologia, evitando anche la dipendenza da internet e dal gioco online.

Un uso controllato e consapevole della tecnologia permette di sfruttarne il pieno potenziale, per questo non si vuole demonizzare Internet o il gioco online, ma orientare gli alunni verso quell'insieme di valori che permettono l'autoregolazione.

Si ricorda a questo proposito che è fondamentale coltivare un dialogo costante con le famiglie. A tal proposito si propongono le indicazioni presenti sulla piattaforma "Generazioni connesse" dal titolo "Comunica con i tuoi figli":

https://www.generazioniconnesse.it/site/it/0000/00/00/comunica-con-i-tuoi-figli/

che consigliano innanzitutto di conoscere, gli adulti per primi, i vari rischi della rete, evidenziarne però anche le potenzialità positive, parlarne di frequente con i figli e stimolarne l'utilizzo proficuo. Stimolare altresì tante attività, anche al di fuori della rete, proporsi come modello da seguire dando per primi l'esempio e servirsi delle limitazioni quali il "Parental control".

4.5 - Sexting

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

Il nostro Istituto vuole fornire al personale della scuola, agli studenti e alle famiglie strumenti finalizzati al riconoscimento e alla prevenzione di tale fenomeno.

Foto e video condivisi online spesso diventano oggetto di una diffusione incontrollabile e ciò può creare seri problemi personali, nonché questioni legali, legati alla persona ritratta e a chi diffonde i contenuti.

Inoltre l'invio di foto o video che riguardano minorenni in pose sessualmente esplicite si configura come reato di distribuzione di materiale pedopornografico.

I contenuti sessualmente espliciti possono diventare anche materiale di ricatto assumendo la forma di "revenge porn", "vendetta porno", ossia diffusione illecita dei contenuti al fine di ricattare chi vi è ritratto.

I rischi del sexting possono comportare: violenza psicosessuale, umiliazione, bullismo, cyberbullismo, molestie, stress emotivo, ansia, sfiducia negli altri, depressione.

I temi del sexting sono trattati anche nei seguenti video che sono consigliati agli studenti delle classi II e III della Scuola Secondaria di Primo grado:

La ragazza visibile - https://www.youtube.com/watch?v=CH4Vz4dDeD8

Se mi posti ti cancello - https://www.youtube.com/watch?v=Kox-8mKZXSo

---

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.

L'Istituto intende fornire agli studenti, alle loro famiglie e ai docenti strumenti finalizzati al riconoscimento e alla prevenzione del fenomeno.

Inoltre intende predisporre percorsi di educazione alla sessualità e all'affettività anche avvalendosi di esperti professionisti specializzati.

La problematica dell'adescamento online si inquadra infatti in uno scenario più ampio di scarsa educazione emotiva, sessuale e di competenza digitale.

Si può rendere gli studenti maggiormente pronti a questo tipo di rischi se sono emotivamente più sicuri e in grado di gestire le proprie emozioni e il rapporto con il proprio corpo e con gli altri.

Gli adulti coinvolti, nelle famiglie, a scuola o nelle associazioni devono poter rappresentare un riferimento nel caso in cui i ragazzi e le ragazze si rivolgano a loro per presentare questo tipo di problemi, anche quando pensano di aver fatto un errore, si vergognano o si sentono in colpa. Il ragazzo o la ragazza deve poter fidarsi di loro e non sentirsi giudicato, ma ascoltato e compreso.

E' importante che gli alunni proteggano e sappiano gestire la propria privacy e la propria identità in rete, nonché le proprie relazioni (il mezzo può permettere di entrare in contatto anche con sconosciuti che possono celare la propria identità).

La piattaforma "Generazioni connesse" suggerisce una serie di video che trattano il tema dell'adescamento online e di altri rischi legati alla rete con un linguaggio rivolto ai giovani, indicato per gli alunni delle classi II e III della scuola Secondaria di Primo grado.

https://www.youtube.com/watch?v=MVzATpbAx3w

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.

Al fine di facilitare la rimozione del materiale dalla rete e di consentire le attività investigative è importante far pervenire quanto prima le segnalazioni agli indirizzi indicati e alla Polizia postale. In questo modo si potrà proteggere maggiormente le vittime di queste azioni e perseguire chi commette reato.

Parallelamente è opportuno, per il benessere delle persone coinvolte, ricorrere a un supporto psicologico rivolgendosi al medico di base, al pediatra o ai servizi socio-sanitari del territorio, come i consultori familiari e i centri specializzati.

Se si viene a conoscenza di tali reati si fa riferimento alla Polizia di Stato - compartimento di Polizia postale e delle comunicazioni.

Il nostro piano d'azioni

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

□ 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 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.

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

Già durante l'a.s. 2019-2020 alcune classi dell'IC hanno potuto partecipare a incontri formativi con l'associazione "Informatici senza frontiere" su rischi e uso consapevole della rete, all'interno del progetto "Liberi...in rete" dell'IC carrarese- euganeo

Le classi terze SSPG plesso A. Moro - Due Carrare- hanno trascorso una mattinata con l'arma dei Carabinieri-sezione di Abano T. per conoscere i rischi dell'uso improprio della rete.

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

☐ 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.

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.

E' importante che i minori o coloro i quali venissero a conoscenza di fatti che riguardano i rischi legati alle tematiche affrontate in questo documento si rivolgano agli insegnanti, ai collaboratori, ai genitori, a figure di riferimento per una tempestiva segnalazione.

In particolare è importante monitorare fatti relativi a:

contenuti afferenti la violazione della privacy: foto o video pubblicati contro la propria volontà, indirizzi, numeri di telefono, ecc.

contenuti afferenti all'aggrestività o alla violenza: minacce, offese, informazioni false, contenuti razzisti, contenuti che inneggiano al suicidio, insulti, foto o video umilianti, ecc.

contenuti afferenti alla sessualità: grooming (adescamento tramite messaggi/comunicazioni di vario genere), pedopornografia, sexting, ecc.

5.2. - Come segnalare: quali strumenti e a chi

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

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

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

- CASO A (SOSPETTO) – Il docente ha il sospetto che stia avvenendo qualcosa tra gli/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.

La segnalazione nell'Istituto può essere effettuata da qualsiasi docente, da genitori/tutori, dagli stessi studenti (nella sucola secondaria) tramite mail all'indirizzo:

aiuto@iccarrareseeuganeo.edu.it

Il referente d'Istituto per il bullismo e il cyberbullismo nell'a.s. 2023/24 è il prof. Andrea Fincato.

Il personale preposto si occupa di raccogliere le informazioni necessarie e a segnalare i fatti al Dirigente Scolastico.

Il Dirigente Scolastico, insieme al personale preposto (team Antibullismo) valuta se la segnalazione debba essere rivolta anche a organi esterni alla scuola quali Polizia Postale, Carabinieri, Servizi sociali o se il caso vada gestito all'interno della scuola secondo il regolamento.

La tipologia di intervento è determinata dalla valutazione approfondita del Team Antibullismo e del dirigente.

Inoltre, a seguito dell'intervento, viene compiuto un monitoraggio per valutarne gli effetti e l'efficacia sia a breve che a lungo termine.

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.

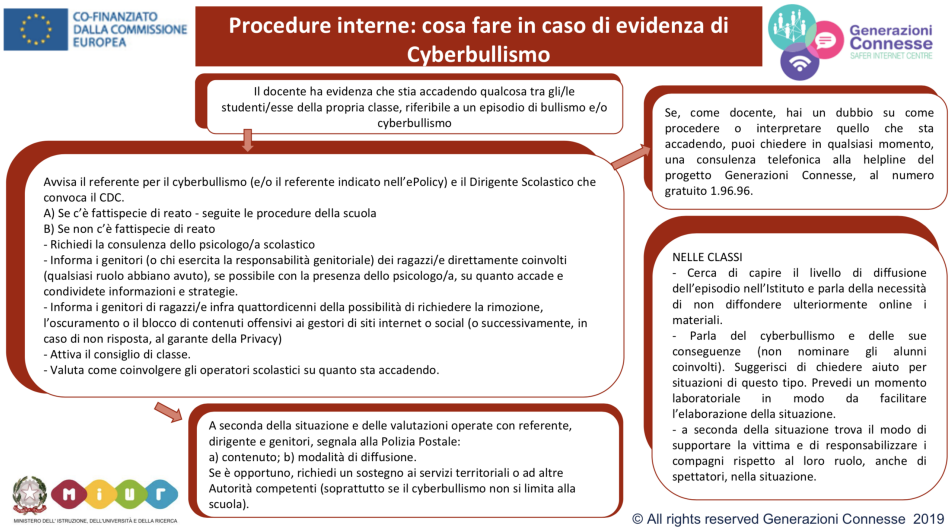
Per una mappatura degli indirizzi di tali strutture è possibile consultare il Vademecum di Generazioni Connesse "Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all'utilizzo delle tecnologie digitali da parte dei più giovani" (seconda parte, pag. 31), senza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

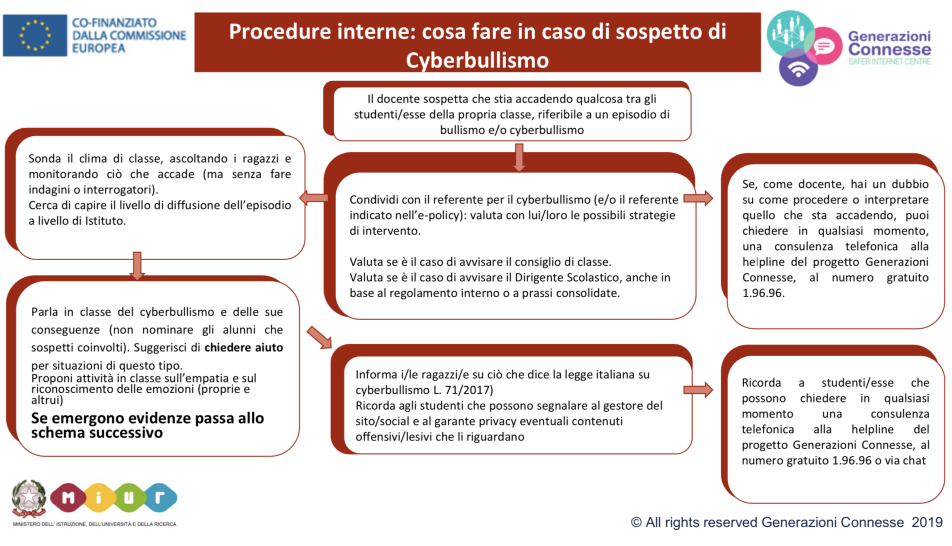
A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all'utilizzo di Internet può presentare.

- **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.

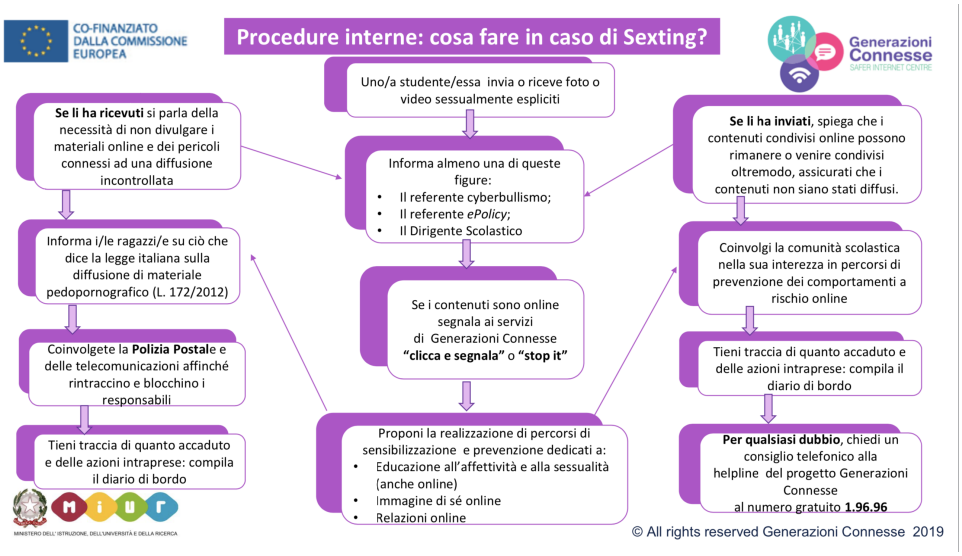
5.4. - Allegati con le procedure

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

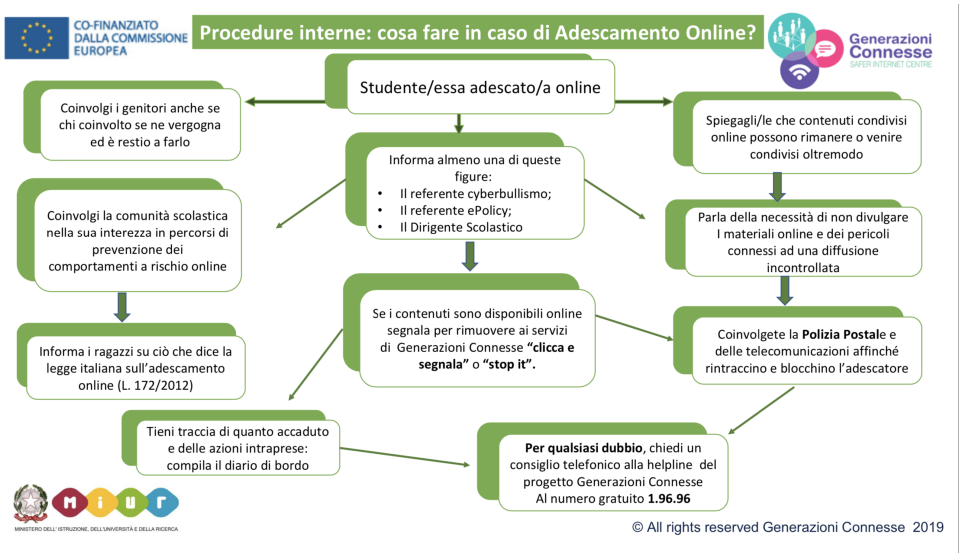




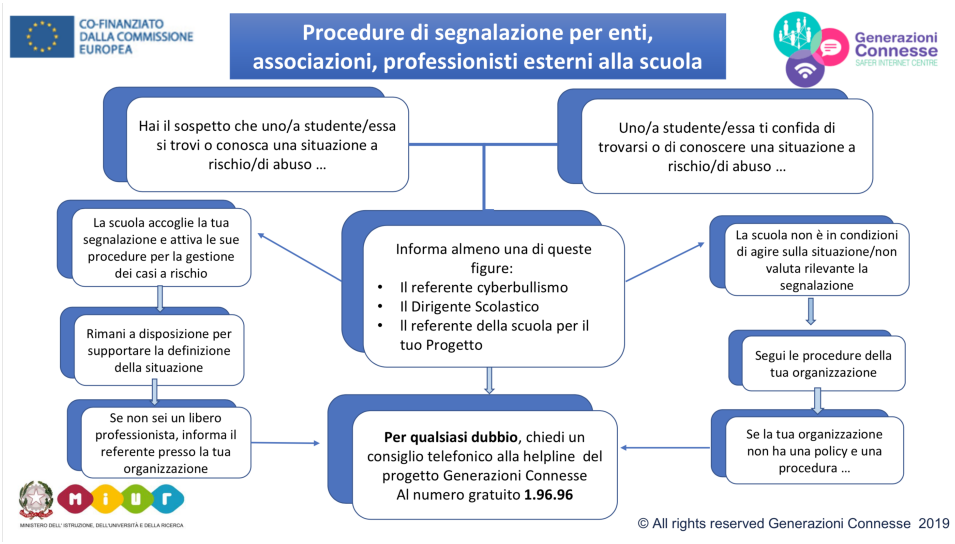
Procedure interne: cosa fare in caso di sexting?



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

Diffusione capillare delle procedure a tutti gli attori coinvolti.