Documento di ePolicy

BRIC82100V

PRIMO I.C. S.VITO DEI NORMANNI

VIA SAN DOMENICO - 72019 - SAN VITO DEI NORMANNI - BRINDISI (BR)

Francesco Dell'Atti

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.

Il nostro Istituto si propone, attraverso il documento dell'ePolicy, di costruire un ecosistema di responsabilità digitale: regole chiare e condivise con l'intera comunità scolastica, con i partner esterni e gli enti che partecipano sinergicamente al processo educativo.

L'evoluzione digitale contribuisce sicuramente a creare un mondo più equo e sostenibile, permettendo una maggiore inclusione e personalizzazione dei percorsi didattici e favorendo un maggiore coinvolgimento e partecipazione da parte degli alunni, "nativi digitali".

Le TIC e l'accesso a Internet dal computer di classe o dai dispositivi personali, pur configurandosi come strumenti atti a favorire l'apprendimento, possono, se utilizzati in modo improprio, costituire fattori di rischio tanto per gli studenti, quanto per gli adulti, "immigrati digitali", che intervengono a vario titolo nel processo educativo. Si ritiene pertanto necessario sviluppare un approccio organico alle tematiche legate alle competenze digitali, alla sicurezza online e ad un uso consapevole delle tecnologie digitali nella didattica, stabilendo norme comportamentali e procedure per l'utilizzo delle tecnologie digitali in ambiente scolastico e individuando misure per la prevenzione, per la rilevazione e gestione delle problematiche connesse ad un uso non consapevole delle tecnologie digitali.

La nostra scuola dispone di un Atelier Digitale finanziato dal PNSD e fruibile da tutti gli ordini. L'Istituto ha inoltre partecipato a due bandi, di seguito riportati, nell'area dei Fondi Strutturali Europei – Programma Operativo Nazionale "Per la scuola – Competenze e ambienti per l'apprendimento" 2014/2020: • Bando 1 - 9035 del 13/07/2015 - FESR - realizzazione/ampliamento rete LanWLan. Il progetto presentato è stato giudicato ammissibile. • Bando 2 - 12810 del 15/10/2015 -FESR – Realizzazione AMBIENTI DIGITALI.

L'Istituto ha partecipato inoltre ai bandi 4878 del 17/04/2020 - FESR - Realizzazione di smart class per la scuola del primo ciclo, 20480 del 20/07/2021 - FESR REACT EU - Realizzazione di reti locali, cablate e wireless, nelle scuole, 28966 del 06/09/2021 - FESR REACT EU - Digital board: trasformazione digitale nella didattica e nell'organizzazione, ottenendo l'autorizzazione al finanziamento per tutte le azioni richieste.

Il "Piano d'Azione" adottato lo scorso anno scolastico ha consentito alla nostra Istituzione scolastica di focalizzare parte del proprio Piano Triennale dell'Offerta Formativa e definire il proprio approccio:

- alle tematiche legate alla legalità, affettività ed alle competenze digitali;
- alla sicurezza online e ad un uso positivo delle tecnologie digitali nella didattica;
- alle norme comportamentali e alle procedure per l'utilizzo delle tecnologie dell'informazione e della comunicazione (ICT) in ambiente scolastico;
- alle misure per la prevenzione;
- alle misure per la rilevazione e gestione delle problematiche connesse a un uso non consapevole delle tecnologie digitali;
- alle iniziative di informazione e di prevenzione del cyberbullismo con il coinvolgimento delle forze dell'ordine;
- alla formazione del personale docente e non sulle competenze digitali e sulla legalità.

Il dettato normativo ha attribuito, a una pluralità di soggetti compiti e responsabilità ben precisi, ribadendo il ruolo centrale della Scuola che è chiamata a realizzare azioni in un'ottica di governance diretta dal MIUR che includano la formazione del personale, la partecipazione di un proprio referente per ogni autonomia scolastica, la promozione di un ruolo attivo degli studenti.

Tra gli obiettivi formativi prioritari, lo sviluppo delle competenze digitali degli studenti con prime conoscenze di coding, finalizzato anche a un utilizzo critico e consapevole dei social network e dei media, come previsto dal Piano Nazionale Scuola Digitale.

La Scuola ha messo in atto le seguenti azioni:

- Protocolli d' intesa con i servizi territoriali (servizi dell'ASL, forze dell'ordine, partenariati con l'Amministrazione e le altre scuole del territorio) in grado di fornire supporto specializzato e continuativo ai minori coinvolti in questo processo di crescita educativa;
- Progetto di Educazione alla cittadinanza;
- progetti di Educazione all'affettività promossi dall'ASL;
- progetti di Educazione alla legalità promossi dalla compagnia dei Carabinieri;
- progetto "Una scuola amica" – UNICEF;
- progetto "Il Consiglio Comunale dei ragazzi";
- progetti promossi dal CONI;
- progetto "Together for a better Internet";
- progetti CLIL: Euro-Techno CLIL, Science Digital CLIL;
- progetto ERASMUS KA226 "CONNECTED BY KNOWLEDGE;
- formazione docenti sul coding (a cura dell'animatore digitale);
- formazione docenti sulle tecnologie e approcci metodologici innovativi;
- formazione docenti sull'insegnamento dell'Educazione Civica.

L'istituto ha aderito, nell'ambito dell'insegnamento di Educazione Civica, per gli as. 2021/2023 al Progetto "Connessioni Digitali" promosso da SAVE THE CHILDREN in collaborazione con il MIUR, il CREMIT dell'Università Cattolica di Milano e la cooperativa EDI ONLUS.

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.

DIRIGENTE SCOLASTICO

Il Dirigente Scolastico è responsabile della sicurezza online insieme al DSGA; garantisce la sicurezza, anche on line, dell'intera comunità scolastica tutelandone i dati; promuove ed organizza corsi di formazione sull'uso delle TIC; gestisce e interviene in caso di bullismo, cyberbullismo ed uso improprio delle TIC; garantisce a scuola l'uso di un Internet Service filtrato approvato, conforme ai requisiti di legge vigenti.

DSGA

Il DSGA è responsabile, unitamente al DS, della sicurezza online; è responsabile nei confronti del personale amministrativo incaricato al trattamento dei dati; promuove la consapevolezza e l'impegno per la salvaguardia online in tutta la comunità scolastica; garantisce che tutto il personale sia a conoscenza delle procedure che devono essere seguite in caso di incidente per la sicurezza online; coordina i vari interventi con le autorità locali e le agenzie competenti; garantisce la tutela dei dati degli alunni pubblicati sul sito della Scuola.

IL PERSONALE AMMINISTRATIVO, TECNICO E AUSILIARIO (ATA)

Il personale ATA concorre, con le proprie mansioni, a garantire la sicurezza online tutelando i dati trattati; conosce e rispetta le procedure da attivare in caso di infrazione.

L'ANIMATORE DIGITALE

L'Animatore digitale promuove percorsi di formazione nell'Istituto e supporta il personale scolastico da un punto di vista tecnico-informatico e sui rischi online.

IL REFERENTE BULLISMO E CYBERBULLISMO

Il Referente ha il compito di promuovere e coordinare iniziative mirate per la prevenzione e il contrasto del bullismo e del cyberbullismo; monitora eventuali azioni di cyberbullismo; pubblica l'ePolicy sul sito della scuola e la diffonde attraverso Power Point e schede; organizza uno o più incontri, avvalendosi del contributo delle forze dell'ordine/polizia postale/enti/associazioni, dedicati alla prevenzione dei rischi associati all'utilizzo di internet e delle tecnologie digitali, rivolti agli studenti, con il

coinvolgimento delle famiglie soprattutto (Cyberbullismo, Sexting, Violazione della Privacy, Adescamento Online, ecc.).

I DOCENTI

I docenti integrano i problemi di sicurezza informatica in tutti gli aspetti del curricolo di studi e in altre attività extracurricolari; condividono le competenze in uscita dei ragazzi; supervisionano e guidano gli alunni impegnati in attività di apprendimento con l'ausilio delle TIC in ambienti online; responsabilizzano gli alunni relativamente ai problemi legali dei contenuti elettronici come ad esempio siti illegali, plagio, leggi sul copyright e relativi problemi di sicurezza online; promuovono e diffondono il regolamento relativo al corretto utilizzo a scuola dei dispositivi elettronici: cellulari, fotocamere, dispositivi portatili; osservano, valutano e segnalano qualsiasi abuso, sospetto o problema ai responsabili della sicurezza online e al D. S, per le opportune indagini/azioni/ sanzioni; mantengono tutte le comunicazioni digitali con alunne/alunni e genitori/tutori a livello professionale realizzandole esclusivamente con sistemi ufficiali scolastici; si formano sull'utilizzo e l'integrazione delle TIC nella didattica, sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali, sulla Gestione dell'infrastruttura e della strumentazione ICT della scuola, sull'accesso ad internet: filtri, antivirus e sulla navigazione.

GLI ALUNNI

Gli alunni conoscono l'ePolicy d'Istituto e applicano le regole per il corretto utilizzo dei dispositivi elettronici/multimediali a scuola; informano immediatamente il docente di qualsiasi abuso e/o messaggio, informazione o pagina che compare sul dispositivo utilizzato che crea disagio; sono consapevoli dei rischi e delle conseguenze, anche penali, per un uso non corretto di Internet e delle altre tecnologie, sia a scuola che a casa (plagio, diritti d'autore, diffusione non autorizzata di dati personali e immagini, atti di cyberbullismo, invio di materiali lesivi, offensivi o inappropriati durante le attività didattiche; riprese non permesse di eventi, fatti e situazioni durante le attività didattiche).

I GENITORI

I genitori accettano l'ePolicy d'Istituto e sostengono la Scuola nel promuovere la sicurezza online; leggono, comprendono e controfirmano il presente accordo inserito nel Patto Educativo di Corresponsabilità; conoscono il Regolamento d'Istituto e i relativi provvedimenti disciplinari da applicare in caso di violazione delle disposizioni stabilite a livello collegiale.

GLI ENTI EDUCATIVI ESTERNI E LE ASSOCIAZIONI

Gli Enti educativi esterni e le associazioni che partecipano al processo educativo con la scuola condividono le regole relative all'uso consapevole della Rete e delle TIC; promuovono comportamenti sicuri, la sicurezza online; assicurano la protezione degli studenti e delle studentesse.

1.3 - Un’informativa per i soggetti esterni che erogano attività educative nell’Istituto

Tutti gli attori che entrano in relazione educativa con gli studenti e le studentesse devono: mantenere sempre un elevato profilo personale e professionale, eliminando atteggiamenti inappropriati, essere guidati dal principio di interesse superiore del minore, ascoltare e prendere in seria considerazione le opinioni ed i desideri dei minori, soprattutto se preoccupati o allertati per qualcosa.

Sono vietati i comportamenti irrispettosi, offensivi o lesivi della privacy, dell’intimità e degli spazi personali degli studenti e delle studentesse oltre che quelli legati a tollerare o partecipare a comportamenti di minori che sono illegali, o abusivi o che mettano a rischio la loro sicurezza.

Tutti gli attori esterni sono tenuti a conoscere e rispettare le regole del nostro Istituto dove sono esplicitate le modalità di utilizzo dei propri dispositivi personali (smartphone, tablet, pc, etc.) e quelli in dotazione della scuola, evitando un uso improprio o comunque deontologicamente scorretto durante le attività con gli studenti e le studentesse. Esiste l’obbligo di rispettare la privacy, soprattutto dei soggetti minorenni, in termini di fotografie, immagini, video o scambio di contatti personali (numero, mail, chat, profili di social network).

L’Istituto, al fine di garantire una sicurezza esaustiva a tutta la comunità scolastica, predispone, per i soggetti esterni che partecipano al processo educativo nell’Istituto, un’informativa contenente:

1. Premessa e obiettivi
2. Destinatari (organizzazioni e soggetti esterni).
3. Ambiti di applicazione (il progetto specifico o delle attività) e Ruoli (individuare i docenti di riferimento del progetto specifico o delle attività).
4. Regolamento / Codice di comportamento.
5. Procedure di segnalazione.
6. Provvedimenti nel caso di omessa segnalazione e/o comportamenti in violazione del codice di comportamento.

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.

L'ePolicy d'Istituto è condivisa con l'intera comunità scolastica attraverso la sua pubblicazione sul sito della scuola, nella sezione del PTOF relativa alla Disciplina del Regolamento di Istituto e nel Banner dedicato al Bullismo e al Cyberbullismo.

Si condivide con la componente studentesca il documento "ePolicy" sin dai primi giorni di scuola con le classi Prime in ingresso coinvolte nel progetto Accoglienza; gli alunni conservano un estratto di questo documento, adattato secondo le diverse fasce d'età, nel diario scolastico con l'indicazione dei comportamenti corretti e di quelli da evitare.

L'ePolicy è condivisa con i genitori all'inizio dell'anno scolastico, allegata al Patto di Corresponsabilità, e nell'ambito di incontri organizzati per sensibilizzare sul tema della sicurezza informatica, per informare e formare circa i comportamenti da monitorare e/o da evitare.

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 alla ePolicy possono essere rilevate da docenti/ATA nell'esercizio delle proprie funzioni oppure possono essere segnalate dagli alunni e dai genitori a docenti e D. S. Qualora esse si configurino come vero e proprio reato, occorre darne tempestiva segnalazione al Dirigente Scolastico per gli adempimenti del caso. Infatti è bene ricordare a tutti che nel momento in cui un qualunque attore della comunità scolastica venga a conoscenza di un reato perseguibile d'ufficio, è fatto obbligo di denuncia (ex art. 331 del codice di procedura penale). L'omissione di denuncia costituisce reato (art. 361). I reati che, in ambiente scolastico, possono essere riferiti all'ambito digitale e commessi per via telematica sono tra gli altri:

 Minaccia, in particolare, se la minaccia è grave, per tale reato si procede d'ufficio (art. 612 codice penale);

 Induzione alla prostituzione minorile (art. 600bis);

 Pedopornografia (art. 600ter);

 Corruzione di minorenne (art. 609quinquies).

Nel caso in cui le infrazioni della ePolicy violino norme previste dal Regolamento di Istituto, si procede secondo quanto previsto dal Regolamento di Disciplina; la scuola eroga delle sanzioni secondo il principio della sensibilizzazione e del risarcimento dell'eventuale danno provocato, in uno spirito di recupero e rieducazione.

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.

Il presente regolamento sarà inserito nella sezione del PTOF relativa alla Disciplina del Regolamento d'Istituto, nella categoria Regolamento d'Istituto del tab PTOF, nel Banner dedicato al bullismo e cyberbullismo.

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 corpo docente, dopo l'approvazione a livello collegiale del documento programmatico, si confronta, sempre in sede collegiale, annualmente, circa la necessità di apportare modifiche e miglioramenti alla ePolicy vigente elaborando eventuali nuovi protocolli di intervento.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

- Realizzazione di un sistema di monitoraggio delle attività.
- Realizzazione di un'assemblea per discutere delle attività di progetto.
- Sensibilizzazione di tutta la Comunità scolastica con il coordinamento e la direzione del TEAM di lavoro (animatore digitale, tre figure del Team per l'innovazione digitale, responsabili dei laboratori d'informatica e due responsabili del Bullismo e Cyberbullismo) per pianificare e attuare misure di prevenzione e gestione di situazioni problematiche relative all'uso delle TIC coinvolgendo anche i genitori.
- Sviluppo dei progetti sull'Educazione Civica, sulla Legalità, sulle competenze digitali, sulla Cittadinanza attiva, sul contrasto al bullismo e cyber bullismo.

Azioni da svolgere nei prossimi 3 anni:

- Analizzare il fabbisogno formativo degli insegnanti sull'uso sicuro della Rete;
- Promuovere la partecipazione dei docenti a corsi di formazione che abbiano ad oggetto i temi del progetto "Generazioni Connesse".
- Monitorare le azioni svolte per mezzo di specifici momenti di valutazione;
- Organizzare incontri con professionisti della scuola o con esperti esterni, enti/associazioni, etc.

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.

La diffusione delle tecnologie di informazione costituisce una vera e propria rivoluzione in quanto interessa tutti i domini dello scibile umano, sempre di più alla portata di tutti alla velocità di un click.

La competenza digitale è infatti una delle otto competenze chiave individuate dall'UE: le soluzioni digitali determinano un'importante accelerazione dei cambiamenti sociali, culturali, ambientali ed economici.

L'Agenda 2030 mette in evidenza come lo sviluppo sostenibile, declinato in vari obiettivi, sia promosso e favorito dalla competenza digitale e dalle meta-competenze, come l'empatia, la resilienza, la creatività, il pensiero critico.

L'Educazione pertanto gioca un ruolo chiave nel nuovo scenario culturale che si sta delineando, non solo perché le competenze richieste nel mondo del lavoro sono in continua evoluzione, ma anche perché, proprio grazie alle tecnologie, cambia il modo

di trasferirle.

Diventa perciò necessario per l'apprendimento costruire un curriculo verticale che porti ogni alunno a sviluppare competenze digitali che gli consentiranno gradualmente una cittadinanza sempre più consapevole, inclusiva, responsabile, attiva e partecipe.

PROFILO DELLE COMPETENZE DIGITALI AL TERMINE DEL PRIMO CICLO DI ISTRUZIONE

Le "Indicazioni per il Curricolo per la Scuola dell'Infanzia e per il primo ciclo di istruzione", emanate con D.M. n.254 del 16/11/2012 gazzetta ufficiale n.30 del 05/02/2013, individuano i traguardi per lo sviluppo delle competenze digitali al termine del primo ciclo: L'alunno … "ha buone competenze digitali, usa con consapevolezza le tecnologie della comunicazione per ricercare e analizzare dati ed informazioni, per distinguere informazioni attendibili da quelle che necessitano di approfondimento, di controllo e di verifica e per interagire con soggetti diversi nel mondo. Utilizza la lingua inglese nell'uso delle tecnologie dell'informazione e della comunicazione". Tenendo presente anche i NUOVI SCENARI 2018, questi traguardi si declinano nelle seguenti Abilità – Conoscenze e Competenze:

CURRICOLI DEL PRIMO CICLO DI ISTRUZIONE - SCUOLA INFANZIA - PRIMARIA E SECONDARIA DI I GRADO – COMPETENZE DIGITALI
Competenze finali: Padroneggiare le abilità e le tecniche di utilizzo delle nuove tecnologie . Utilizzare le nuove tecnologie con autonomia e responsabilità nel rispetto degli altri, prevenendo ed evitando i pericoli

SCUOLA DELL'INFANZIA

TRAGUARDI ATTESI IN USCITA	ABILITÀ	CONOSCENZE
Utilizzare le nuove tecnologie per giocare, svolgere compiti, acquisire informazioni, con la supervisione dell'insegnante.	Muovere correttamente il mouse e i suoi tasti. Utilizzare i tasti delle frecce direzionali, dello spazio, dell'invio Individuare e aprire icone relative a comandi, file, cartelle … Individuare e utilizzare, su istruzioni dell'insegnante, il comando "salva" per un documento già predisposto e nominato dal docente stesso. Eseguire giochi ed esercizi di tipo logico, linguistico, matematico, topologico, al computer. Prendere visione di lettere e forme di scrittura attraverso il computer. Prendere visione di numeri e realizzare numerazioni utilizzando il computer Utilizzare la tastiera alfabetica e numerica una volta memorizzati i simboli. Visionare immagini, opere artistiche, documentari.	l computer e i suoi usi Mouse Tastiera Icone principali di Windows e di Word Altri strumenti di comunicazione e i suoi usi (audiovisivi, telefoni fissi e mobili….)

SCUOLA PRIMARIA

TRAGUARDI ATTESI IN USCITA	ABILITÀ	CONOSCENZE

	Utilizzare strumenti informatici e di comunicazione per elaborare dati, testi e immagini e produrre documenti in diverse situazioni. Conoscere gli elementi basilari che compongono un computer e le relazioni essenziali fra di essi. Collegare le modalità di funzionamento dei dispositivi elettronici con le conoscenze scientifiche e tecniche acquisite. Utilizzare materiali digitali per l'apprendimento Utilizzare il PC, periferiche e programmi applicativi. Utilizzare la rete per scopi di informazione, comunicazione, ricerca e svago. Riconoscere potenzialità e rischi connessi all'uso delle tecnologie più comuni, anche informatiche.	Il sistema operativo e i più comuni software applicativi, con particolare riferimento all'office automation e ai prodotti multimediali anche Open source. Procedure per la produzione di testi, ipertesti, presentazioni e utilizzo dei fogli di calcolo. Procedure di utilizzo di reti informatiche per ottenere dati, fare ricerche, comunicare. Caratteristiche e potenzialità tecnologiche degli strumenti d'uso più comuni. Procedure di utilizzo sicuro e legale di reti informatiche per ottenere dati e comunicare (motori di ricerca, sistemi di comunicazione mobile, email, chat, social network, Gsuite for Education e app, protezione degli account, download, diritto d'autore, ecc.). Fonti di pericolo e procedure di sicurezza.
Utilizzare con dimestichezza le più comuni tecnologie dell'informazione e della comunicazione, individuando le soluzioni potenzialmente utili ad un dato contesto applicativo, a partire dall'attività di studio. Essere consapevole delle potenzialità, dei limiti e dei rischi dell'uso delle tecnologie dell'informazione e della comunicazione, con particolare riferimento al contesto produttivo, culturale e sociale in cui vengono applicate.		
FINE SCUOLA SECONDARIA DI I GRADO		
TRAGUARDI ATTESI IN USCITA	ABILITÀ	CONOSCENZE

	Area 1 Alfabetizzazione su informazione e dati Identificare siti web, blog e database digitali, accedervi e navigare per scopi di informazione e ricerca.	
	Utilizzare la rete per scopi di informazione e ricerca .	
	Padroneggiare azioni e procedure per aprire e usare programmi e applicativi.	Caratteristiche e potenzialità tecnologiche degli strumenti d'uso più comuni.
	Esplorare e selezionare i diversi programmi applicativi.	
		Procedure di utilizzo della rete per ottenere dati, fare ricerche.
	Area 2 Comunicazione e collaborazione Rilevare la credibilità e l'affidabilità delle fonti comuni di dati, informazioni e contenuti digitali.	Sistemi operativi e software applicativi anche OER di maggiore diffusione.
	Organizzare, archiviare e recuperare con facilità dati, informazioni e contenuti negli ambienti digitali.	Siti, blog, database comunemente utilizzati poiché credibili e affidabili, Fake news.
	Riconoscere dove organizzarli in modo semplice in un ambiente strutturato.	
	Condividere dati, informazioni e contenuti digitali e per l'interazione.	App, procedure per l'archiviazione di URL e link relativi a siti web, ai blog e ai database digitali, cronologia.
Utilizzare con dimestichezza le più comuni tecnologie dell'informazione e della comunicazione, individuando le soluzioni potenzialmente utili ad un dato contesto applicativo, a partire dall'attività di studio.	Identificare adeguati mezzi di comunicazione semplici per un determinato contesto.	Chat di uso comune (WhatsApp, Facebook, Messenger, classe virtuale, G Suite for Education e sue app, Forum)
	Area 3 Creazione di contenuti digitali Utilizzare strumenti informatici per produrre testi, ipertesti, ritoccare e/o adattare immagini e creare prodotti multimediali.	Procedure per la produzione di testi, ipertesti, disegni, audiovideo, presentazioni, storytelling e utilizzo dei fogli di calcolo.
Essere consapevole delle potenzialità, dei limiti e dei rischi dell'uso delle tecnologie dell'informazione e della comunicazione, con particolare riferimento al contesto produttivo, culturale e sociale in cui vengono applicate.	Utilizzare strumenti informatici per salvare ed organizzare documenti in cartelle e sottocartelle.	Procedure di programmazione (coding).
	Area 4 Sicurezza Usare i vari dispositivi informatici e della comunicazione in modo corretto.	Procedure di utilizzo sicuro e legale di reti informatiche per ottenere dati e comunicare (motori di ricerca, sistemi di comunicazione mobile, e-mail, chat, social network, protezione degli account, download, diritto d'autore, l'uso Common Creative, ecc.)
	Effettuare correttamente download e upload. Creare, gestire e rinnovare la password personale. Effettuare correttamente login e logout.	Norme di comportamento per la pubblicazione di testi, immagini e video propri o di altri.
	Effettuare correttamente connessione e disconnessione. Conoscere e rispettare le regole del copyright.	Rischi, fonti di pericolo e procedure di sicurezza sia per la salute che per il benessere psicofisico. Netiquette
	Riconoscere potenzialità e rischi connessi all'uso delle tecnologie più comuni, anche informatiche.	Piattaforme di apprendimento e supporti IT.
	Area 5 Risolvere problemi Individuare semplici problemi tecnici nell'utilizzo dei dispositivi e delle tecnologie digitali.	
	Identificare semplici soluzioni per risolverli. Individuare esigenze, riconoscere semplici strumenti digitali e possibili risposte tecnologiche per soddisfarli. Scegliere semplici modalità per adattare e personalizzare gli ambienti digitali alle esigenze personali.	Giochi educativi, personalizzazione dell'interfaccia, profilo.

Il nostro Istituto, come previsto dal PTOF, promuove l'apprendimento del coding, cioè la programmazione informatica, per abituare ad un'informatica maker, oltre che consumer. Partendo perciò da un'alfabetizzazione digitale, si arriverà allo sviluppo del pensiero computazionale, essenziale affinché le nuove generazioni siano in grado di affrontare la società e le tecnologie del futuro, non come consumatori passivi, ma come utenti attivi.

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.

La legge 107/2015, al comma 124, definisce la formazione in servizio del personale docente come "obbligatoria, permanente e strutturale" in coerenza con il piano triennale dell'offerta formativa e il PDM, sulla base dei bisogni emersi e delle priorità nazionali indicate nel Piano nazionale di formazione.

La competenza digitale, oggi, è imprescindibile per i docenti così come per studenti e studentesse e permette di integrare la didattica con strumenti che la diversificano, la rendono innovativa e in grado di venire incontro ai nuovi stili di apprendimento.

Il nostro Istituto, come si evince dal RAV e dal PDM, promuove lo sviluppo delle competenze digitali degli studenti, con particolare riguardo al pensiero computazionale, all'utilizzo critico e consapevole dei social network e dei media nonché alla produzione e ai legami con il mondo del lavoro. promuove l'uso delle TIC nella didattica e la formazione digitale continua del personale docente.

La formazione interna alla scuola sui temi del PNSD è organizzata dall'Animatore Digitale, col supporto del TEAM digitale, al fine di favorire la partecipazione e stimolare il protagonismo degli studenti nell'organizzazione di workshop e altre attività, anche aprendo i momenti formativi alle famiglie e ad altri attori del territorio, per la realizzazione di una cultura digitale condivisa.

Sono previsti Progetti CLIL per le classi della SSPG da svilupparsi attraverso le TIC e attività di CODING.

La SSPG partecipa inoltre al Progetto ERasmus+ KA226 "Connected by knowledge" che mira a potenziare le competenze digitali degli alunni in Lingua Inglese, attraverso attività di mobilità nei Paesi Partner (Spagna, Lituania e Grecia) e attività online su piattaforma eTwinning e GSUITE.

L'Istituto ha inoltre ottenuto l'Accreditamento per il Programma Erasmus+ 2021-2027 e il finanziamento per azioni che mirano allo sviluppo e al potenziamento delle competenze di cittadinanza digitale attraverso attività di Job Shadowing e corsi di formazione rivolti ai docenti e mobilità di gruppo studenti.

La formazione esterna prevede la partecipazione dei docenti ai progetti realizzati dalle scuole in relazione all'adesione alla rete dell'ambito n.12 della provincia di Brindisi.

E' prevista inoltre la partecipazione a seminari, convegni, corsi on-line organizzati dagli Enti del territorio, dalle scuole in rete che partecipano al PNSD, da esperti interni alla scuola che rientreranno nell'organico di potenziamento e da esperti esterni a pagamento; tali interventi saranno rivolti:

· ai docenti tutti e a quelli che avranno un profilo di accesso personale al sito, con il quale contribuiranno ad alimentare i contenuti didattici dello stesso;

· al personale amministrativo, dotato di un profilo di accesso personale al sito, che gestirà la comunicazione delle circolari, il registro elettronico e il personale;

· ai collaboratori scolastici, in primo piano nella comunicazione con gli utenti della scuola;

· alle famiglie, destinatarie di servizi on line;

Il processo è in corso e riguarda gli anni scolastici 2020-2022.

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.

Le piattaforme di apprendimento, le classi virtuali, le App e i software educativi sostengono docenti ed alunni nell'utilizzo consapevole e sicuro di internet e delle TIC. È tuttavia necessario che gli insegnanti si formino e si aggiornino sui rischi della RETE per prevenire e contrastare ogni forma di discriminazione, offesa, denigrazione e lesione della dignità dell'altro, nonché fenomeni di bullismo e cyberbullismo.

Il nostro Istituto ha previsto per tutte le classi della SSIG e le classi della Scuola Primaria, che richiedano un intevento specifico, nell'ambito del progetto "**Together for a better internet...from all over Europe** ", momenti di formazione a cura della Referente d'Istituto Bullismo e cyberbullismo, rivolti all'intera comunità scolastica con l'ausilio delle forze dell'ordine, della Polizia Postale, della Polizia di Stato; la celebrazione del SID, in collaborazione con i Partner del Progetto Erasmus+ "Connected by knowledge": il nostro Istituto si occuperà di sviluppare l'unità di apprendimento "INTERNET: A SAFE PLACE TO LEARN"; la condivisione nel Banner preposto sul sito della scuola di link e materiali informativi e strumenti per la valutazione, la rilevazione e il monitoraggio di eventuali atti di bullismo e/o cyberbullismo, modelli per reclamo GDPR per docenti, alunni e genitori.

I docenti dei tre ordini ed alcuni genitori parteciperanno ai corsi offerti dalla Piattaforma SIC.

La Referente di Istituto seguirà l'aggiornamento proposto da Generazioni Connesse, la formazione proposta dal Progetto "Connessioni Digitali", ulteriori corsi proposti eventualemente dalla piattaforma ELISA.

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.

Con riferimento a quanto previsto dalla legge 29.5.2017, n.71 e le nuove Linee di orientamento per la prevenzione e il contrasto del cyberbullismo (nota MIUR n. 482 del 18.2.2021), alla famiglia spetta l'obbligo/l'impegno a vigilare e educare i propri figli con riferimento alla prevenzione dei fenomeni di bullismo e cyberbullismo ed alla Scuola l'impegno a prevenire e a contrastare il bullismo e il cyberbullismo, promuovendo la conoscenza e la diffusione delle LINEE GUIDA per la prevenzione e contrasto al Bullismo e Cyberbullismo, delle regole relative al rispetto tra gli studenti, alla tutela della loro salute, alla corretta comunicazione e al corretto comportamento sul web, vigilando sulla condotta degli studenti e dotandosi, attraverso formazione continua dei Dirigenti Scolastici, della Referente d'istituto e del TEAM antibullismo, sulla Piattaforma Generazioni Connesse ed ELISA, di strumenti idonei per il contrasto al Bullismo e Cyberbullismo.

La docente Referente si impegna a diffondere le Nuove Linee di Orientamento che comprendono:

- Indicazione di strumenti utili e buone pratiche per contrastare i fenomeni del bullismo e cyberbullismo:

- Focus sul Progetto Safer Internet Centre-Generazioni Connesse;

- Analisi degli aspetti relativi alla formazione in modalità e-learning dei docenti referenti (Piattaforma ELISA - E-learning degli Insegnanti sulle Strategie Anti bullismo);

- Indicazioni di procedure operative per elaborare azioni efficaci, individuate a loro volta, in "prioritarie" e "consigliate";

- Possibili modelli di prevenzione su più livelli (universale-selettiva e indicata) ed esempi di implementazione degli stessi;

- Invito a costituire Gruppi di Lavoro (Team Antibullismo e Team per l'Emergenza) a livello scolastico e territoriale, integrati all'occorrenza da figure specialistiche di riferimento, ricorrendo ad eventuali reti di scopo;

- Suggerimenti di protocolli d'intervento per un primo esame dei casi d'emergenza;

- Ricognizione delle iniziative e impegni degli organi collegiali e del personale scolastico;

- Uso di spazi web dedicati sui siti scolastici istituzionali in ottica di diffusione e rilancio della cultura del rispetto dell'altro;

- Appendice con modello fac-simile di segnalazione di reato o situazioni di rischio ad altri organi competenti.

Il nostro piano d'azioni

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

L'Istituto prevede di sviluppare nel corso dell'anno scolastico 2021/2022 le seguenti Azioni:

- Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Coinvolgere una rappresentanza dei genitori per individuare i temi di maggiore interesse nell'ambito dell'educazione alla cittadinanza digitale.
- Sviluppare buone pratiche nell'ambito dell'utilizzo corretto delle TIC.
- Scambio di buone pratiche con le scuole Partner del progetto Erasmus+ "CONNECTED BY KNOWLEDGE".
- Organizzare workshop, nell ambito del progetto Erasmus+ "Connected by Knowledge", rivolti a docenti, studenti e famiglie.

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

3.1 - Protezione dei dati personali

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

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

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

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

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

In questo paragrafo dell'ePolicy affrontiamo tale problematica, con particolare

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

In riferimento al dlgs 30 giugno 2003, n. 196 (c. d. Codice della Privacy) e al nuovo Regolamento europeo Privacy n. 679/2016, il nostro Istituto individua delle Linee Guida che disciplinano il trattamento dei dati personali gestiti:

- Predisposizione e condivisione con l'intera comunità scolastica di un'informativa che illustri il ruolo del DPO, la tipologia di dati raccolti, il loro utilizzo e il fine per cui vengono utilizzati;
- All'atto dell'iscrizione è richiesto alle famiglie di firmare un'autorizzazione scritta per consentire l'uso didattico di immagini e video;
- Pubblicazione sul sito istituzionale di fotografie o video di gruppo;
- I nomi completi di alunne e alunni non saranno pubblicati sul sito web come pure nei blog, forum e wiki, in particolare se in associazione con le loro fotografie;
- Predisposizione di una liberatoria specifica per la condivisione di immagini e video durante eventi a carattere pubblico particolarmente rilevanti;
- Predisposizione di una liberatoria specifica per la condivisione di elaborati ai fini della partecipazione a concorsi, a eventi pubblici;
- Predisposizione di liberatorie specifiche, contenenti le modalità di trattamento, la conservazione dei dati raccolti e le misure di sicurezza adottate, per la somministrazione di questionari di ricerca e per la partecipazione ad attività che coinvolgono personale esterno alla scuola;
- Messa a disposizione dei genitori sul sito istituzionale del modello di reclamo al Garante per la protezione dei dati personali in caso di violazioni in materia di cyberbullismo;
- Regolamentazione sull'uso di dispositivi in grado di registrare e di strumenti compensativi previsti nei PdP/PEI.

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.

Secondo il Piano Nazionale Scuola Digitale (PNSD) , adottato con Decreto Ministeriale n. 851 del 27 ottobre 2015, la sfida dell'educazione nell'era digitale parte dall'accesso.

Il PNSD prevede interventi specifici, promossi e coordinati dall'Animatore Digitale, in merito alla formazione degli insegnanti, al miglioramento delle dotazioni hardware, alle attività didattiche.

Per quanto riguarda la formazione, l'animatore promuove la partecipazione a seminari, convegni, corsi on-line organizzati dagli Enti del territorio, dalle scuole in rete che partecipano al PNSD, da esperti interni alla scuola che rientrano nell'organico di potenziamento e da esperti esterni a pagamento.

Tali interventi sono rivolti:

· ai docenti tutti e a quelli che hanno un profilo di accesso personale al sito, con il

quale contribuiscono ad alimentare i contenuti didattici dello stesso;

· al personale amministrativo, dotato di un profilo di accesso personale al sito, che gestirà la comunicazione delle circolari, il registro elettronico e il personale;

· a tutti i docenti in possesso dell' account @primocomprensivosanvito.edu.it;

· ai collaboratori scolastici, in primo piano nella comunicazione con gli utenti della scuola;

· alle famiglie, destinatarie di servizi on line.

L'animatore inoltre, attraverso il ricorso a video tutorial, fornisce supporto a docenti, personale ATA e famiglie, relativamente all'uso corretto di GSUITE e le APP della piattaforma di apprendimento.

Il processo è in corso di attuazione e riguarda gli anni scolastici dal 2020 al 2022.

In merito all'implementazione della dotazione hardware, il progetto presentato per il Bando 1 - 9035 del 13/07/2015 - FESR - realizzazione/ampliamento rete LanWLan, è stato giudicato ammissibile, quello per il Bando 2 - 12810 del 15/10/2015 -FESR – Realizzazione AMBIENTI DIGITALI.

L'autorizzazione al Progetto 4878 del 17/04/2020 - FESR - Realizzazione di smart class per la scuola del primo ciclo, ha permesso di allestire una smart class nella Scuola Primaria.

Il finanziamento ottenuto grazie al bando DM 48 permette di allestire il laboratorio scientifico ed altri spazi della SSIG "Don V. Meo" con arredi, monitor interattivi e centraline metereologiche.

L'autorizzazione al Progetto 28966 del 06/09/2021 - FESR REACT EU - Digital board: trasformazione digitale nella didattica e nell'organizzazione, permetterà di acquistare ulteriori strumenti digitali.

L'Istituto attualmente grazie alla partecipazione ai bandi PON è dotato di una rete wireless destinata all' utilizzo didattico da parte del corpo docente e degli alunni che utilizzano gli IPad in dotazione nell'Atelier Creativo. La password è unica a livello di Istituto. Ciascun utente connesso alla rete dovrà: rispettare il presente regolamento e la legislazione vigente succitata, tutelare la propria privacy, quella degli altri utenti adulti e degli alunni al fine di non divulgare notizie private contenute nelle documentazioni elettroniche cui ha accesso.

L'autorizzazione al Progetto 20480 del 20/07/2021 - FESR REACT EU - Realizzazione di reti locali, cablate e wireless, nelle scuole, permetterà di implementare la connessione di due plessi del nostro Istituto.

L'adesione al Progetto "Connessioni Digitali", nell'ambito dell'insegnamento dell'Educazione civica, ha consentito al nostro Istituto di allestire una Newsroom

presso la sede della SSPG "Don V. Meo".

Al fine di garantire la safety nell'accesso ad Internet gli studenti saranno guidati allo sviluppo di competenze digitali per un uso consapevole delle TIC e della RETE e al rispetto della "netiquette" (insieme di regole, comunemente accettate e seguite da quanti utilizzano Internet e i servizi di rete, che disciplinano il comportamento di un utente nel rapportarsi agli altri utenti attraverso risorse come wiki, newsgroup, mailing list, forum, blog o e-mail).

L'Istituto si è dotato di una PUA: norme di buon utilizzo che la scuola si impegna a redigere e a divulgare prima che sia concesso l'accesso a Internet alla componente studentesca (NETIQUETTE , uso corretto della piattaforma GSUITE FOR EDUCATION, Regolamento Didattica Integrata).

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

- Mantenere separate la rete didattica e la segreteria: importante per garantire maggiore sicurezza alle informazioni, gestendo in modo autonomo e con regole differenti le due reti grazie al firewall.
- Aggiornare periodicamente software e Sistema operativo: garantire che il sistema sia aggiornato per proteggerlo dalle aggressioni esterne e dalle vulnerabilità che emergono nel tempo.
- Definire la programmazione di backup periodici: cioè la copia e messa in sicurezza dei dati del sistema scolastico per prevenire la perdita degli stessi (possibilmente anche una copia offline).
- Garantire formazione adeguata allo staff, incluso il corpo docenti: la formazione deve riguardare la gestione dei dispositivi, la conoscenza delle regole basilari sulla sicurezza.
- Testare regolarmente le possibili vulnerabilità.
- Preparare piani di azione in risposta ai problemi più seri: avere un protocollo di azione.
- Predisporre la disconnessione automatica dei dispositivi, dopo un certo tempo di inutilizzo: se non è previsto uno stand-by, il dispositivo resta accessibile nel caso in cui qualcuno dimentichi di spegnerlo, con il rischio potenziale di accesso da parte di persone non autorizzate.
- Impostare il browser per l'eliminazione dei cookies alla chiusura: in questo modo si evita che qualcuno possa avere accesso ad account altrui senza autorizzazione.
- Definire una policy sulle password.
- Adottare sistemi di filtraggio software e hardware o servizi specifici forniti d Internet provider per bloccare contenuti dannosi o materiali non adatti.

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 DS coordina la comunicazione interna ed esterna del nostro Istituto a partire da un piano di comunicazione in grado di trasmettere all'esterno l'identità, i valori, le azioni, i progetti e l'idea di educazione che la scuola porta avanti. Sono stati individuati alcuni docenti responsabili del Sito Web e della pagina FB di Istituto. Altri mezzi di comunicazione online in dotazione alla scuola sono: il registro elettronico con tutte le sue funzionalità, lo sportello di segreteria digitale, la mail, strumenti di messaggistica istantanea come whatsapp (docenti-genitori esclusivamente per fini didattici), ulteriori applicativi e piattaforme di lavoro condiviso e collaborativo come G Suite for Education, eTwinning.

Il registro elettronico consente una comunicazione chiara e immediata con le famiglie relativamente a:

1. andamento scolastico (assenze, argomenti lezioni e compiti, note disciplinari);
2. risultati scolastici (voti, documenti di valutazione);
3. comunicazione varie (comunicazioni di classe, comunicazioni personali).

I colloqui individuali per gli incontri SCUOLA-FAMIGLIA e i ricevimenti settimanali dei docenti sono organizzati attraverso Calendar di GSUITE.

Tutte le comunicazioni scuola-famiglia contenenti dati sensibili sono visibili da parte della famiglia dell'alunno interessato e non dal resto della classe. Solo il DS e i docenti del CDC possono avere accesso a tali informazioni.

Il riepilogo delle medie con relative valutazioni ed eventuali assenze è accessibile sul registro elettronico AXIOS dal profilo dei Coordinatori di classe.

3.4 - Strumentazione personale

I dispositivi tecnologici sono parte integrante della vita personale di ciascuno, compresa quella degli/lle studenti/esse e dei docenti (oltre che di tutte le figure professionali che a vario titolo sono inseriti nel mondo della scuola), ed influenzano

necessariamente anche la didattica e gli stili di apprendimento. Comprendere il loro utilizzo e le loro potenzialità innovative, diventa di cruciale importanza, anche considerando il quadro di indirizzo normativo esistente e le azioni programmatiche, fra queste il Progetto Generazioni Connesse e il più ampio PNSD.

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

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

Il Primo Istituto Comprensivo di San Vito dei Normanni dispone il divieto dell'utilizzo del cellulare o di altri dispositivi elettronici per uso personale. È consentito il loro utilizzo previa autorizzazione scritta dei docenti indicante data e ora. Tale divieto deriva dai doveri sanciti dallo Statuto delle Studentesse e degli Studenti (D.P.R. n. 249/1998 come modificato dal D.P.R. n. 235/2007 e successivi). La violazione di tale divieto configura un'infrazione disciplinare rispetto alla quale la scuola è tenuta ad applicare apposite sanzioni.

Sia alunni (quando autorizzati dal docente) e i docenti sono tenuti a spegnere i propri cellulari prima dell'ingresso in aula.

Il nostro piano d'azioni

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

- Organizzare uno o più eventi o attività volti a formare il personale dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali.
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali.
- Organizzare uno o più eventi o attività volti a formare i genitori dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali.
- Organizzare uno o più eventi o attività volti a formare il personale dell'Istituto sui temi dell'accesso ad Internet e dell'uso

sicuro delle tecnologie digitali (cybersecurity).

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

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

4.1 - Sensibilizzazione e Prevenzione

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

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

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

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

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

Nell'ambito delle attività di sensibilizzazione, il nostro Istituto ha previsto incontri con le forze dell'ordine, con i Carabinieri, con la Polizia Postale e di Stato. Sono stati inoltre programmati, come interventi di prevenzione universale, dei momenti di formazione destinati ai genitori ed agli alunni delle classi della Scuola Secondaria di primo grado e la celebrazione del Safer Internet Day. I genitori sono stati altresì

invitati a svolgere la formazione offerta dalla piattaforma SIC di Generazioni Connesse.

Le misure di prevenzione comprendono l'integrazione nel curricolo dei temi legati al corretto utilizzo delle TIC e di Internet. A tal proposito l'offerta formativa del nostro Istituto contempla progetti curriculari ed extra-curriculari che hanno tra le priorità l'utilizzo critico e consapevole dei social network e dei media e lo sviluppo di competenze di digitali e di cittadinanza attiva: "**Together for a better internet...from all over Europe**", **eTwinning** - **ERASMUS+ "Connected by knowledge"**, "**Connessioni Digitali**" **,** partecipazione alla **settimana Europea del Coding**.

In tutti e tre gli ordini, tra le iniziative previste per il futuro, ci sarà la promozione di lezioni con l'obiettivo di insegnare agli studenti della scuola il coding, cioè la programmazione informatica, per abituare ad un'informatica maker, oltre che consumer. Partendo perciò da un'alfabetizzazione digitale, si arriverà allo sviluppo del pensiero computazionale, essenziale affinché le nuove generazioni siano in grado di affrontare la società e le tecnologie del futuro, non come consumatori passivi, ma come utenti attivi.

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 nostro Istituto ha previsto azioni mirate alla prevenzione e contrasto di atti di cyberbullismo, come definito dalla legge 71/2017, art. 1, comma 2 e secondo quanto indicato nelle Linee di orientamento per la prevenzione e il contrasto del cyberbullismo.

La Referente per il contrasto al bullismo e cyberbullismo ha seguito la formazione su Generazioni Connesse, quela prevista dalla piattaforma ELISA e sta attualmente svolgendo formazione relativa al progetto "Connessioni Digitali". La Referente d'istituto è inoltre Referente per ERASMUS+ e svolge formazione INDIRE e eTwinning.

La prevenzione universale e l'uso corretto delle TIC sono altresì promosse dal Progetto ERASMUS+ KA226 "Connected by knowledge" e dal piano di internazionalizzazione del nostro Istituto relativo all'accreditamento ERASMUS+ 2021-2027.

La docente Referente è inoltre responsabile del BANNER sul sito istituzionale per la lotta al bullismo e al cyberbullismo e si occupa di aggiornarlo periodicamente con strumenti, moduli, materiali da mettere a disposizione dell'intera comunità scolastica.

In colaborazione con la FS territorio, la docente Referente organizza incontri con il territorio al fine di sensibilizzare e prevenire atti che si configurano come bullismo e cyberbullismo nel nostro Istituto, inclusi, con le relative sanzioni comminate dai rispettivi organi competenti., nel Regolamento di Istituto e nel patto di corresponsabilità.

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.

I progetti "**Together for a better internet...from all over Europe**" e "**Connected by knowledge**" si occuperanno di approfondire aspetti legati al Cyberbullismo e il fenomeno dell'HATE SPEECH.

Saranno organizzate, nell'ambito di questi Progetti, attività di riconoscimento di Hate Speech e si inviteranno gli alunni ad attività di riflessione sulla componente discriminatoria propria dell'HATE SPEECH.

L'HATE SPEECH troverà ampia trattazione nelle UDA trasversali di Educazione Civica destinate alle classi III della SSPG relativamente allo sviluppo delle competenze in materia di cittadinanza digitale.

Attraverso il Progetto di educazione alla cittadinanza si svilupperanno presso gli alunni le competenze in materia di cittadinanza attiva e democratica attraverso la valorizzazione dell'educazione interculturale, il rispetto delle differenze e il dialogo tra le culture, il sostegno dell'assunzione di responsabilità, nonché della solidarietà e della consapevolezza dei diritti e dei doveri. La partecipazione ai vari progetti compresi nel progetto di educazione alla cittadinanza promuoveranno la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network e favoriranno una presa di parola consapevole e costruttiva da parte dei giovani.

4.4 - Dipendenza da Internet e gioco online

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

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

La tecnologia ha modificato gli ambienti in cui viviamo e ha un impatto sulla qualità della vita. Pertanto si rende necessario, nell'ambito dei Progetti offerti dal Nostro Istituto e destinati allo sviluppo delle competenze digitali, affrontare il problema della dipendenza da Internet e promuovere presso gli alunni:

- la ricerca di equilibrio nelle relazioni anche online;
- l'uso degli strumenti digitali per il raggiungimento di obiettivi personali;
- la capacità di interagire negli ambienti digitali in modo sicuro e responsabile;
- la capacità di gestire il sovraccarico informativo e le distrazioni (ad esempio, le notifiche);
- la capacità di scegliere contenuti adatti alla propria età e di segnalare quelli non adatti;
- la capacità di gestire il tempo di connessione.

Sarà fatta informazione sul fatto che ciò può rappresentare una vera e propria patologia che compromette la salute e le relazioni sociali e che in taluni casi (per es. uso della carta di credito a insaputa di altri) rappresenta un vero e proprio illecito. Le tecnologie e il gioco online rendono l'apprendimento accattivante, motivante e divertente, quindi il riconoscimento, la condivisione e il rispetto di alcune regole fondamentali si pone come necessario per poter ricorrere a queste risorse.

Le regole individuate e condivise all'interno di ogni classe, il Regolamento di Istituto, i contenuti che saranno sviluppati durante la formazione offerta a genitori ed alunni mirano proprio a dotare adulti e ragazzi di riferimenti normativi e conoscenze utili per l'utilizzo consapevole e sicuro delle TIC.

4.5 - Sexting

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

Tra gli atti che si configurano come cyberbullismo vi è il sexting: l’invio e/o ricezione di messaggi contenenti video o immagini a sfondo sessuale.

Tra le caratteristiche di questo fenomeno ci sono:

- la fiducia tradita di chi ha inviato tramite messaggi video o immagini sessualmente espliciti, su richiesta del destinatario, come prova d’amore;
- la pervasività con cui si diffondono i contenuti e il rischio di pedopornografia;
- la permanenza nel tempo dei contenuti.

La Legge 19 luglio 2019 n. 69, all’articolo 10 ha introdotto in Italia il reato di Revenge Porn, con la denominazione di diffusione illecita di immagini o di video sessualmente espliciti.

Il nostro Istituto, al fine di fornire agli studenti le conoscenze dei rischi legati ad un utilizzo improprio dei social, si occuperà di differenziare la formazione offerta agli studenti, calibrando l'intervento educativo in base alla fascia d'età.

La Scuola inoltre si prefigge di informare i genitori circa le possibilità di attivare forme di controllo parentale.

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.

La nostra scuola si propone di sensibilizzare genitori e alunni sull'esistenza di individui che usano la rete per instaurare relazioni, virtuali o reali, con minorenni e per indurli alla prostituzione.

La Referente d'Istituto svolgerà interventi educativi mirati nelle classi della Scuola Primaria che ne facciano richiesta, sui rischi che comporta l'uso scorretto di alcuni social anche da parte di adulti (TikTok, WhatsApp, Facebook, Instagram) e relativi alla Privacy, all'adescamento. Nel corso di questi interventi saranno proiettati video spot della Polizia di Stato ed altri video della serie "I SUPERRORI" di Generazioni Connesse.

L'adescamento sarà inoltre trattato in occasione del SID con interventi e approfondimenti da parte delle Forze dell'Ordine e della Polizia di Stato/Postale.

4.7 - Pedopornografia

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

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

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

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

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

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

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

Il nostro Istituto, attraverso le attività di formazione, intende sensibilizzare e prevenire fenomeni legati all'uso inconsapevole delle TIC e dei social, tra i quali anche il sexting e la pedopornografia.

Il Dirigente Scolastico, a tal proposito, promuove i servizi offerti da Generazioni Connesse, per la formazione e informazione dei genitori e del personale docente, ed attività di sensibilizzazione e prevenzione al fine di mettere a conoscenza la comunità scolastica della Legge 71/2017 sul cyberbullismo, della normativa in materia di Codice Penale e Civile relativamente ad atti che si configurano come cyberbullismo.

Il nostro piano d'azioni

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

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

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

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

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

AZIONI (da sviluppare nell'arco dei prossimi anni scolastici)

- 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 extra-scolastici, sui temi della diversità e sull'inclusione rivolti a genitori, studenti/studentesse e personale della scuola.

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

Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

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

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

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

Nelle procedure:

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

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

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

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

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

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

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

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

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

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

Vi suggeriamo, inoltre, i seguenti servizi:

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

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

segnalare la presenza di materiale pedopornografico online.

Il nostro Istituto ha previsto un protocollo d'azione nel caso in cui si verifichino atti che si configurano come Bullismo e Cyberbullismo: harassment, denigration, exclusion, impersonation, exposure, trickery, cyberstalking, sexting, grooming.

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.

Sul sito del nostro Istituto, nel Banner appositamente dedicato al contrasto al Bullismo e Cyberbullismo (https://primocomprensivosanvito.edu.it/pagina.asp?art=307), sono a disposizione di docenti, alunni e famiglie diversi materiali e strumenti: il modello di reclamo al Garante per la protezione dei dati personali per il blocco, rimozione e oscuramento di qualsiasi dato personale del minore diffuso illecitamente nella RETE.

Il modulo di prima segnalazione, approvato in sede collegiale, sarà affiancato dal modulo di valutazione approfondita.

La prima segnalazione sarà presa in carico dall'insegnante che rileva il caso di presunto bullismo o cyberbullismo. Successivamente il team di emergenza valuterà la situazione e, qualora il comportamento rilevato rappresenti un vero e proprio illecito, informerà immediatamente il DS che convocherà le famiglie degli alunni interessati per gli adempimenti del caso.

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.

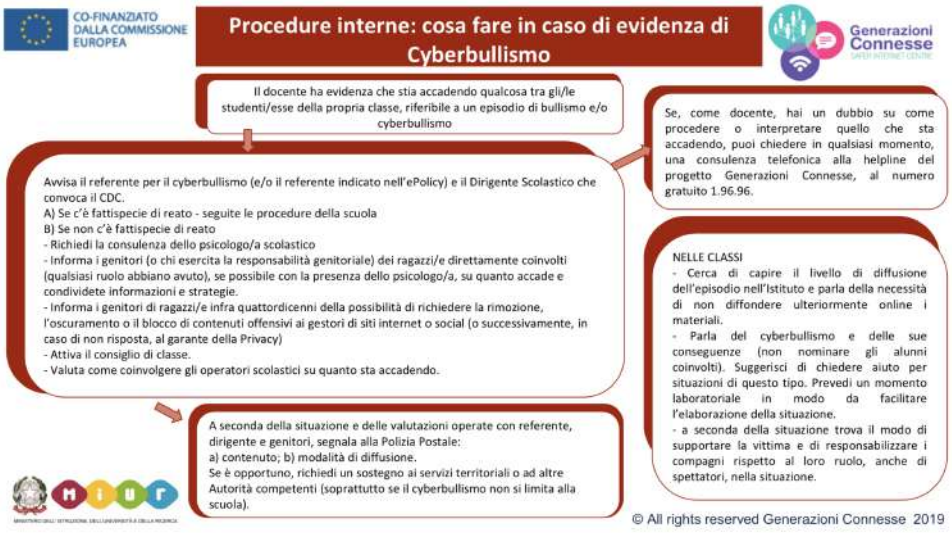
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni)**: svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare attenzione alla tutela dei minori.
- **Ufficio Scolastico Regionale**: supporta le scuole in attività di prevenzione ed anche nella 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.

Nelle attività di sensibilizzazione e prevenzionae universale è indispensabile coinvolgere altri attori sul Territorio.

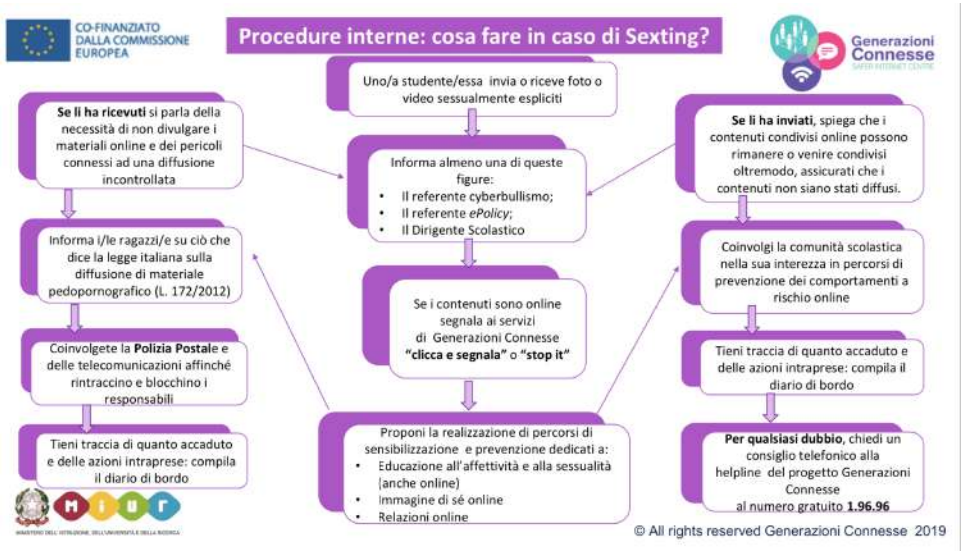
Il nostro Istituto collabora da anni con le forze dell'ordine. I carabinieri, annualmente, offrono, nell'ambito del progetto Bullismo e Cyberbullismo e del progetto Legalità, il proprio supporto agli studenti della Scuola Primaria e Secondaria di primo grado.
Anche la Polizia Municipale, la Polizia di Stato e quella Postale sono coinvolte in attività di sensibilizzazione e prevenzione, in collaborazione con l'ente comunale.

5.4. - Allegati con le procedure

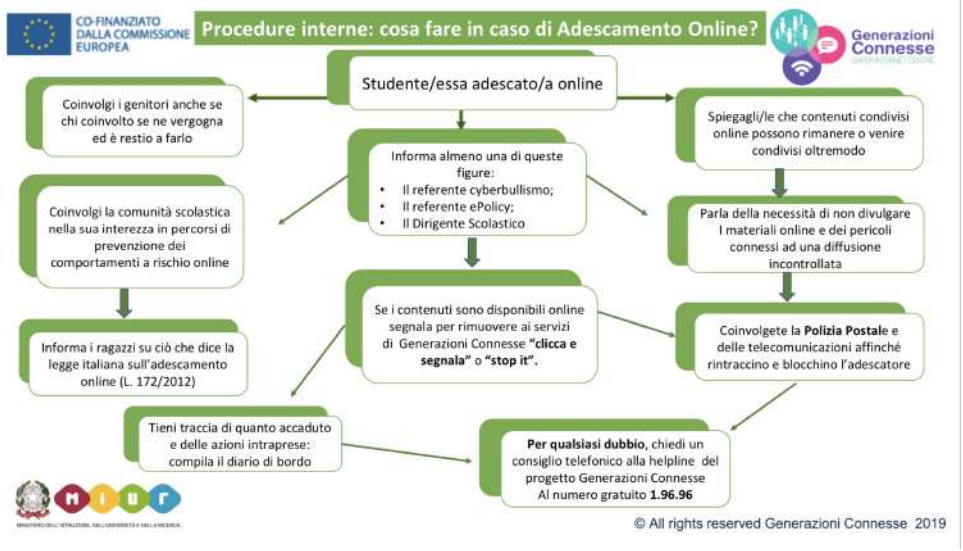
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



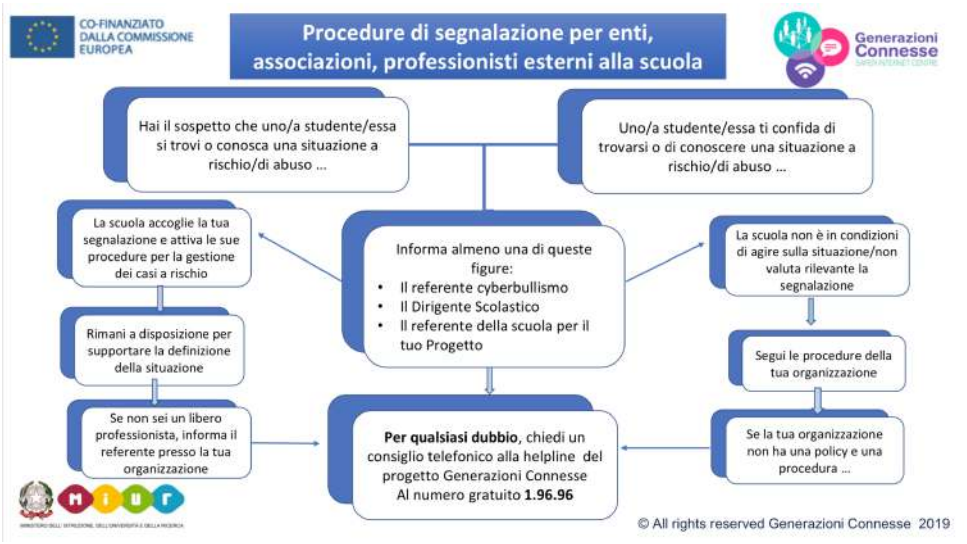
Procedure interne: cosa fare in caso di sexting?



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

Sono stati messi a disposizione dell'intera comunità scolastica nel banner per la lotta al bullismo e cyberbullismo https://primocomprensivosanvito.edu.it/pagina.asp?art=307 :

- il modello di reclamo/segnalazione cyberbullismo al GDPR https://primocomprensivosanvito.edu.it/public/art/generalemodello_per_la_segnalazione_reclamo__in_materia_di_cyberbullismo_(1)_(1).pdf
- il modello di prima segnalazione dei casi di presunto bullismo e vittimizzazione https://primocomprensivosanvito.edu.it/public/art/generaleprima_segnalazione_dei_casiprimoic.pdf

Allegati alla presente ePolicy i seguenti documenti per la DAD:

Netiquette e Social Network

Il Regolamento delle Videoconferenze

Regolamento piattaforma Gsuite

Il nostro piano d'azioni

L'istituto, in collaborazione con l'Ente Comunale, le forze dell'Ordine, la polizia di Stato, la Polizia Postale, l'ASL continuerà a svolgere attività di formazione/informazione rivolta all'intera comunità scolastica al fine di prevenire e contrastare atti che si configurano come Bullismo e Cyberbullismo.