

Via Achille Grandi, 35 - 53041 Asciano (Si) - Tel.: 0577/718357 - Fax: 0577/719074 C.M. SIIC814003 - C.F. 92031340521 www.icpertini.gov.it - e-mail: siic814003@istruzione.it - siic814003@pec.istruzione.it

**E-Safety Policy**

Misure atte a facilitare e promuovere l'utilizzo positivo delle TIC nella didattica e negli ambienti scolastici.

Misure di prevenzione e misure di gestione di situazioni problematiche relative all'uso delle tecnologie digitali.

Indice

Capitolo 1 Introduzione al documento di ePolicy

1.1 - Scopo dell’ePolicy

1.2 - Ruoli e responsabilità

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

1.4 - Condivisione e comunicazione dell’ePolicy all’intera comunità scolastica

1.5 - Gestione delle infrazioni alla ePolicy

1.6 - Integrazione dell’ePolicy con Regolamenti esistenti

1.7 - Monitoraggio dell’implementazione della ePolicy e suo aggiornamento

CAPITOLO 2 Formazione e curricolo

2.1- Curricolo sulle competenze digitali per gli studenti

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

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

2.4 - Sensibilizzazione delle famiglie e integrazioni al Patto di Corresponsabilità

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

3.1 - Protezione dei dati personali

3.2 - Accesso ad Internet

3.3- Strumenti di comunicazione online

3.4 - Strumentazione personale

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

4.1 - Sensibilizzazione e Prevenzione

4.2 - Cyberbullismo: che cos’è e come prevenirlo

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

4.4 - Dipendenza da Internet e gioco online

4.5 – Sexting

4.6 - Adescamento online

**Capitolo 1 Introduzione al documento di 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 l’Istituto Scolastico dotarsi di una ePolicy, un documento programmatico volto a promuovere le competenze digitali ed un uso delle tecnologie positivo, critico e consapevole, sia da parte dei ragazzi e delle ragazze che degli adulti coinvolti nel processo educativo. L’ ePolicy, inoltre, vuole essere un documento finalizzato a prevenire situazioni problematiche e a riconoscere, gestire, segnalare e monitorare episodi legati ad un utilizzo scorretto degli strumenti.

L’ ePolicy 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.

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

**1.1 - Scopo dell’ePolicy**

Scopo del presente documento è quello di informare l’utenza per un uso corretto e responsabile delle apparecchiature informatiche collegate alla rete in dotazione alla Scuola, nel rispetto della normativa vigente.

Gli utenti, siano essi docenti o alunni, devono essere pienamente consapevoli dei rischi a cui si espongono quando navigano in rete. Di fatto esiste la possibilità che durante il lavoro online si possa entrare accidentalmente in contatto con materiale inadeguato e/o illegale, pertanto la Scuola promuove l’adozione di strategie che limitino l’accesso a siti e/o applicazioni illeciti. In questo contesto, gli insegnanti hanno la responsabilità di guidare gli studenti nelle attività online a scuola e di indicare regole di condotta chiare per un uso critico e consapevole di Internet anche a casa, per prevenire il verificarsi di situazioni potenzialmente pericolose.

Le strategie previste dalla scuola per garantire la sicurezza in rete sono le seguenti:

- avvio di percorsi di formazione per un uso consapevole delle TIC rivolti agli insegnanti nel corso dell’anno scolastico;

- coinvolgimento dei genitori come partner educativi nei percorsi di formazione che riguardano gli studenti;

- controllo (una tantum e/o all’evenienza di episodi dubbi) del sistema informatico (cronologia, cookies, ecc.) da parte dei responsabili;

-installazione di firewall sull’accesso Internet;

- presenza di un docente o di un adulto responsabile durante l’utilizzo di Internet, della piattaforma o di altre TIC;

- aggiornamento periodico del software antivirus e scansione delle macchine in caso di sospetta presenza di virus;

-utilizzo di dispositivi esterni e personali, solo se autorizzati.

**1.2 - Ruoli e responsabilità**

Affinché l’ePolicy 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. È opportuno che nel documento vengano definiti con chiarezza ruoli, compiti e responsabilità di ciascuna delle figure all’interno dell’Istituto. È importante specificarlo per ciascuna delle figure professionali che si occupano di gestione e programmazione delle attività formative, didattiche ed educative dell’Istituto e di tutte quelle figure appartenenti alla comunità educante, ovvero:

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

2. l’Animatore digitale supporterà il personale scolastico da un punto di vista non solo tecnico-informatico, ma anche in riferimento ai rischi online, alla protezione e gestione dei dati personali, oltre che essere uno dei promotori di percorsi di formazione interna all’Istituto negli ambiti di sviluppo della “scuola digitale” (con riferimento, ad esempio, allo sviluppo delle competenze digitali previste anche nell’ambito dell’educazione civica); potrebbe, inoltre, monitorare e rilevare eventuali episodi o problematiche connesse all’uso delle TIC a scuola, e avere il compito di controllare che gli utenti autorizzati accedano alla Rete della scuola con apposita password, per scopi istituzionali e consentiti (istruzione e formazione);

3. il Referente bullismo e cyberbullismo avrà il compito di coordinare e promuovere iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo. A tal fine, può avvalersi della collaborazione delle Forze di polizia, delle associazioni e dei centri di aggregazione giovanile del territorio. Fondamentale, dunque, il suo ruolo non solo in ambito scolastico ma anche in quello extrascolastico, in quanto (ove possibile) potrebbe coinvolgere, con progetti e percorsi formativi ad hoc, studenti, colleghi e genitori;

4. il docente ha un ruolo centrale nel diffondere la cultura dell’uso responsabile delle TIC e della Rete e nel libero esercizio della sua professionalità può avvalersi dei seguenti strumenti: postazioni PC, LIM nelle classi e nei laboratori. Inoltre, deve:

-illustrare ai propri alunni le regole di utilizzo contenute nel presente documento;

-dare chiare indicazioni sul corretto utilizzo della rete (Internet, piattaforma studenti ecc.),

-condividere con gli alunni la netiquette e indicanrne le regole;

-assumersi la responsabilità di segnalare prontamente eventuali malfunzionamenti o danneggiamenti al tecnico informatico;

-non divulgare le credenziali di accesso agli account (username e password) e/o, nel caso ne sia a conoscenza, alla rete Wi-Fi;

-non allontanarsi dalla postazione lasciandola incustodita, se non prima di aver effettuato la disconnessione;

-non salvare sulla memoria locale della postazione di classe file contenenti dati personali e/o sensibili;

-proporre agli alunni attività di ricerca di informazioni in rete fornendo opportunamente loro indirizzi dei siti e/o parole chiave per la ricerca cui fare riferimento.

5. Il personale Amministrativo, Tecnico e Ausiliario (ATA) svolge funzioni miste, ossia di tipo amministrativo, contabile, gestionale e di sorveglianza connesse all’attività delle istituzioni scolastiche, in collaborazione con il Dirigente Scolastico e con il personale docente tutto. Diverse figure che, in sinergia, si occupano ciascuno per la propria funzione, del funzionamento dell’Istituto scolastico che passa anche attraverso lo sviluppo della cultura digitale e dell’organizzazione del tempo scuola. Esiste, cioè, un concreto coinvolgimento del personale ATA nell’applicazione della legge 107/15 (“La Buona Scuola”) che concerne non solo il tempo scuola e il potenziamento dell’offerta formativa, ma anche le attività di formazione e autoformazione in tema di bullismo e cyberbullismo. Il personale ATA è, all’interno dei regolamenti d’Istituto, coinvolto nella segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo, insieme ad altre figure e nel raccogliere, verificare e valutare le informazioni inerenti possibili casi di bullismo/cyberbullismo;

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

7. I genitori, in collaborazione con il nostro Istituto scolastico, si renderanno partecipi e attivi nelle attività di promozione ed educazione sull’uso consapevole delle TIC e della Rete, nonché sull’uso responsabile dei device personali; dovrebbero relazionarsi in modo costruttivo con i docenti sulle linee educative che riguardano le TIC e la Rete e comunicare con loro circa i problemi rilevati quando i/le propri/e figli/e non usano responsabilmente le tecnologie digitali o Internet. È estremamente importante che accettino e condividano questo documento di ePolicy e che esiste una corresponsabilità educativa e formativa che riguarda sia i genitori che la scuola nel percorso di crescita degli studenti e delle studentesse (1° comma dell’art. 30 della Costituzione).

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

Gli Enti educativi esterni e le associazioni che entrano in relazione con la scuola dovranno conformarsi alla politica della stessa riguardo all’uso consapevole della Rete e delle TIC; dovranno, inoltre, promuovere comportamenti sicuri, la sicurezza online e assicurare la protezione degli studenti e delle studentesse durante le attività che si svolgono insieme. Per un approfondimento sui ruoli e le responsabilità delle figure presenti a scuola cfr. Legge 59/97, Art. 21 c. 8; Legge N.165/2001, Art. 25; CCNL; DPR n. 275/99; Legge n.107/2015; Piano Nazionale Scuola Digitale.

**1.4 - Condivisione e comunicazione dell’ePolicy all’intera comunità scolastica**

Allo scopo di condividere regole comuni per l’utilizzo sicuro di Internet sia a casa che a scuola, si invitano tutti i genitori a prestare la massima attenzione ai principi e alle regole contenute nel presente documento. Si richiede che ogni genitore e/o tutore si impegni a farle rispettare ai propri figli anche in ambito domestico, primariamente assistendo i minori nel momento dell’utilizzo della rete e poi ponendo in atto tutti i sistemi di sicurezza che aiutino a diminuire il rischio di imbattersi in materiale indesiderato.

L'Istituto si impegna a pubblicare sul sito della scuola il presente documento e prevede di:

1) Condividere e comunicare la politica di e-safety agli alunni:

- tutti gli alunni saranno informati che la rete, l'uso di Internet e di ogni dispositivo digitale saranno controllati dagli insegnanti e utilizzati solo con la loro autorizzazione;

- l'istruzione degli alunni riguardo all'uso responsabile e sicuro di Internet precederà l'accesso alla rete;

- sarà data particolare attenzione nell'educazione sulla sicurezza agli aspetti per i quali gli alunni risultano più esposti o rispetto ai quali risultano più vulnerabili.

2)Condividere e comunicare la politica di e-safety al personale:

-la linea di condotta della scuola in materia di sicurezza nell'utilizzo delle tecnologie digitali e di Internet sarà comunicata formalmente a tutto il personale con il presente documento e altro materiale informativo anche sul sito web;

-un'adeguata informazione/formazione on-line del personale docente sull'uso sicuro e responsabile di Internet, sia professionalmente che personalmente, sarà fornita a tutto il personale, anche attraverso il sito web della scuola;

-tutto il personale è consapevole che una condotta non in linea con il codice di comportamento dei pubblici dipendenti e i propri doveri professionali è sanzionabile.

3)Condividere e comunicare la politica di e-safety ai genitori:

-l'attenzione dei genitori sulla sicurezza nell'uso delle tecnologie digitali e di Internet sarà attirata nelle news o in altre aree del sito web della scuola;

-sarà incoraggiato un approccio di collaborazione nel perseguimento della sicurezza nell'uso delle TIC e di Internet in occasione degli incontri scuola-famiglia, assembleari, collegiali e individuali;

-i docenti di classe forniranno ai genitori indirizzi sul web relativi a risorse utili per lo studio e a siti idonei ed educativi per gli alunni, sistemi di filtraggio e attività educative per il tempo libero.

**1.5 - Gestione delle infrazioni alla ePolicy**

Per la componente alunni, le infrazioni verranno sanzionate come da Regolamento di Istituto pubblicato sul sito web della scuola. Il Dirigente Scolastico ha la facoltà di revocare l'accessibilità temporanea o permanente ai laboratori informatici e/o all'utilizzo di strumenti tecnologici (pc, tablet, notebook, ecc.) a chi non si attiene alle regole stabilite.

In genere, sono previsti da parte dei docenti provvedimenti "disciplinari" proporzionati all'età e alla gravità del comportamento, quali:

- il richiamo verbale;

- il richiamo verbale con particolari conseguenze (riduzione o sospensione dell'attività gratificante);

- il richiamo scritto con annotazione sul diario;

- la convocazione dei genitori da parte degli insegnanti;

- la convocazione dei genitori da parte del Dirigente Scolastico.

I genitori sono invitati a supportare la scuola per mettere a punto azioni di contrasto efficaci. Per la componente docenti, le infrazioni alla ePolicy saranno gestite direttamente dal Dirigente Scolastico.

Qualora le infrazioni alla ePolicy si configurino come vero e proprio reato, occorre darne tempestiva segnalazione al Dirigente Scolastico per gli adempimenti del caso. Si ricorda, infatti, 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).

Per i reati sessuali la magistratura di norma procede su querela di parte; tuttavia nei casi più gravi si persegue d'ufficio e in genere i reati verso le/i minori sono tra quelli per i quali si procede d'ufficio.

**1.6 - Integrazione dell’ePolicy con Regolamenti esistenti**

La presente ePolicy si integra pienamente con il Piano Triennale dell'Offerta Formativa, il Regolamento interno di Istituto e il Patto di Corresponsabilità.

**Testo personalizzato - 1.7 - Monitoraggio dell’implementazione della ePolicy e suo aggiornamento**

Il monitoraggio dell'implementazione della ePolicy sarà compito del Referente per le attività di prevenzione e contrasto del bullismo e cyberbullismo. Si avranno inoltre degli aggiornamenti, laddove necessario e secondo una logica di condivisione e partecipazione attiva, sentito il parere degli insegnanti e viste le esigenze delle famiglie.

**CAPITOLO 2 Formazione e curricolo**

**2.1. Curricolo sulle competenze digitali per gli studenti**

L'Istituto persegue, relativamente al curricolo digitale, le recenti indicazioni del PNSD:

"*Definire le competenze di cui i nostri studenti hanno bisogno è una sfida ben più ampia e strutturata di quella che il sentire comune sintetizza nell'uso critico della Rete, o nell'informatica. Dobbiamo affrontarla partendo da un'idea di competenze allineata al ventunesimo secolo: fatta di nuove alfabetizzazioni, ma anche e soprattutto di competenze trasversali e di attitudini da sviluppare. In particolare, occorre rafforzare le competenze relative alla comprensione e alla produzione di contenuti complessi e articolati anche all'interno dell'universo comunicativo digitale, nel quale a volte prevalgono granularità e frammentazione. Proprio per questo è essenziale lavorare sull'alfabetizzazione informativa e digitale (information literacy e digital literacy), che mettono al centro il ruolo dell'informazione e dei dati nello sviluppo di una società interconnessa basata sulle conoscenze e l'informazione. È in questo contesto che occorre guardare alle sfide rappresentate dal rapporto fra pubblico e privato, dal rapporto tra creatività digitale e artigianato, e tra imprenditorialità digitale, manifattura e lavoro. Ed è ancora in questo contesto che va collocata l'introduzione al pensiero logico e computazionale e la familiarizzazione con gli aspetti operativi delle tecnologie informatiche. In questo paradigma, gli studenti devono essere utenti consapevoli di ambienti e strumenti digitali, ma anche produttori, creatori, progettisti. E i docenti, dalla loro parte e in particolare per quanto riguarda le competenze digitali, dovranno essere messi nelle giuste condizioni per agire come facilitatori di percorsi didattici innovativi basati su contenuti più familiari per i loro studenti*".

Inoltre si fa riferimento alle Indicazioni Nazionali del 2012, che riportano la definizione delle competenze-chiave (Raccomandazione del Parlamento Europeo e del Consiglio del 18 dicembre 2006 - 2006/962/CE) in ambito digitale:

"*La competenza digitale consiste nel saper utilizzare con dimestichezza e spirito critico le tecnologie della società dell'informazione per il lavoro, il tempo libero e la comunicazione. Essa implica abilità di base nelle tecnologie dell'informazione e della comunicazione (TIC): l'uso del computer per reperire, valutare, conservare, produrre, presentare e scambiare informazioni nonché per comunicare e partecipare a reti collaborative tramite Internet*".

Nello specifico, il Curricolo è un percorso formativo, con traguardi da raggiungere strada facendo, che occorre adeguatamente pianificare. Si deve tener conto di obblighi dati dal raggiungimento di obiettivi e di strategie didattiche per l’apprendimento nelle varie età. La progressione didattica relativa al Coding va sviluppata in verticale dalla più tenera infanzia fino all’Università e anche oltre, in riferimento all’apprendimento lungo tutto l’arco della vita (lifelong learning). La diffusione del Coding si espande in un compendio di progettazione e pianificazione trans-curricolare che investe tutte le discipline.

Il Coding, che può essere oggi insegnato attraverso piattaforme disponibili come **code.org**, va studiato e capito non tanto per formare dei professionisti della programmazione, bensì perché la conoscenza dei fondamenti contribuisce a formare il bagaglio tecnico scientifico e culturale di ogni persona. Esso, pertanto, assume nell’insegnamento una duplice funzione: da un lato ha un ruolo culturale formativo di base sul piano scientifico, accompagnando la matematica e le altre scienze e dall’altro quello di strumento trasversale a tutte le discipline che favorisce lo sviluppo logico del pensiero, un approccio curioso di fronte alla realtà e la capacità di provare a risolvere i problemi o di ripartire dagli errori o dagli ostacoli incontrati nei processi formativi.

Nella Scuola dell'Infanzia, attraverso il Coding, si cerca di trasmettere ai cosiddetti “nativi digitali” sia il linguaggio della programmazione e degli algoritmi (mettendo in primo piano la logica che sta dietro alla tecnologia) sia la potenza della segmentazione di un problema e il loro affidamento a piccoli gruppi. Così si dà forza al lavoro collaborativo, al rispetto delle diverse idee.

La costruzione di questa competenze può contribuire a favorire lo sviluppo di elementi di progettualità anche in ambiti disciplinari diversi da quello informatico. Coding e pensiero computazionale rendono possibile apprendere strategie di risoluzione di problemi, progettazione e comunicazione anche a chi non programmerà mai. Grazie alle attività che si possono svolgere nel progetto “**Programma Il Futuro**”, consistenti in esercizi “guidati” sul pensiero computazionale (svolti sia in un ambiente tecnologico, con l’utilizzo del computer e della rete internet sia in modalità “unplugged”), alle attività proposte in **Code Week** e la conoscenza di altri ambienti di programmazione visuale (non è necessario scrivere i comandi, le “stringhe” di codice, ma bisogna mettere in sequenza logica le raffigurazioni grafiche che li rappresentano) come Blockly è possibile acquisire alcune capacità come capire cos’è un algoritmo (facendo scoprire ai bambini che sono algoritmi alcuni dei modi di operare, nella vita di tutti i giorni o a scuola, che realizziamo (quasi) automaticamente), usare il ragionamento logico per spiegare il funzionamento di alcuni semplici algoritmi, capire i principi alla base del funzionamento di un computer, selezionare, trasportare e lasciare (attività di drag and drop).

Nella Scuola Primaria il Coding è una prima forma di approccio interdisciplinare alle TIC: consente l’avvio all’uso consapevole del computer per comprendere che le dotazioni tecnologiche sono strumenti attraverso i quali realizzare dei progetti; sviluppa il pensiero riflessivo e procedurale; stimola la riflessione sull’errore come nuovo spunto di lavoro; sviluppa le capacità di analisi sul proprio operato; incrementa le capacità di espressione linguistica sia orale che scritta per comunicare il proprio operato agli altri o come memoria personale (relazione fasi attività, documento di sintesi del lavoro, etc.); garantisce un utilizzo diretto di conoscenze matematiche, linguistiche, antropologiche e scientifiche per sostanziare di contenuti gli elaborati prodotti; sviluppa il lavoro cooperativo e le abilità individuali. L’obiettivo è di sviluppare tutte queste competenze e capacità attraverso lo studio dei principali costrutti del Coding (iterazione, istruzioni condizionali, funzioni). L’utilizzo di strumenti didattici a difficoltà progressiva, come ad esempio il portale code.org, è fortemente consigliato, sia per le attività al pc sia per quelle unplugged e la piattaforma **Scratch**.

Nella Scuola Secondaria di Primo Grado il pensiero computazionale è un processo mentale per far risolvere problemi ad un agente, sia esso persona o macchina, fornendogli una serie di istruzioni che deve eseguire in autonomia. L’obiettivo è di sviluppare il pensiero computazionale, attraverso l’utilizzo dei costrutti più complessi della programmazione, per la realizzazione di algoritmi ottimizzati ed efficaci per la risoluzione di problemi e attraverso la robotica educativa. Ovviamente, come per la matematica alle medie non si insegna il calcolo differenziale (e non lo si fa neanche alle superiori) così per l'informatica bisogna insegnare i concetti di base in modo adatto allo specifico livello di maturazione degli studenti, ed in modo indipendente dalla tecnologia. L’utilizzo di strumenti didattici a difficoltà progressiva, come ad esempio il portale **code.org,** è indispensabile ad introdurre alcuni concetti piuttosto astratti, come ad esempio le funzioni con parametri. La prosecuzione delle attività con ambienti di programmazione visuali, quali **Scratch o App Inventor**, consentono agli alunni di ideare e realizzare qualcosa di proprio, come ad esempio un videogioco. L’utilizzo infine di supporti legati alla robotica educativa, consentono di ridurre il livello di astrazione e di applicare gli algoritmi realizzati alla programmazione di oggetti che interagiscono con il mondo reale (intelligenza delle cose).

**2.2 - Formazione dei docenti sull’utilizzo e l’integrazione delle TIC (Tecnologie dell’Informazione e della Comunicazione) nella didattica**

Il comma 124 della Legge n. 107/2015 dispone: "*Nell'ambito degli adempimenti connessi alla funzione docente, la formazione in servizio dei docenti di ruolo è obbligatoria, permanente e strutturale. Le attività di formazione sono definite dalle singole istituzioni scolastiche in coerenza con il piano triennale dell'offerta formativa e con i risultati emersi dai piani di miglioramento delle istituzioni scolastiche previsti dal regolamento di cui al decreto del Presidente della Repubblica 28 marzo 2013, n. 80, sulla base delle priorità nazionali indicate nel Piano nazionale di formazione, adottato ogni tre anni con decreto del Ministro dell'istruzione, dell'università e della ricerca, sentite le organizzazioni sindacali rappresentative di categoria.*"

Il corpo docente parteciperà a corsi di formazione nell'ambito di piani nazionali, oltre che ad iniziative organizzate dall'istituzione e dall’ambito territoriale. Il percorso complesso della formazione specifica dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica può prevedere momenti di autoaggiornamento, momenti di formazione personale o collettiva di carattere permanente, legata all'evoluzione rapida delle tecnologie e delle modalità di comunicazione a cui accedono sempre di più ed autonomamente anche i ragazzi.

**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 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.

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

Le famiglie saranno informate della ePolicy e di tutte le azioni che la scuola promuove e condivideranno questo documento all'inizio dell'anno scolastico, unitamente al Patto di corresponsabilità. Inoltre, potranno consultare, sul sito istituzionale della scuola, materiale relativo all'utilizzo delle TIC, tra cui la piattaforma "Generazioni Connesse".

La scuola avrà cura di sensibilizzare le famiglie, attraverso documentazione informativa ed incontri, ad un corretto uso delle nuove tecnologie da parte dei ragazzi a casa e a scuola, indicando anche alcune semplici azioni che possono rendere la navigazione sicura. In modo particolare, per quanto concerne l'accesso alle attrezzature disponibili in classe (LIM e computer portatile) e nei laboratori, informerà sui regolamenti e la normativa vigente. Inoltre, promuoverà l'uso delle nuove tecnologie al fine di assicurare un valore aggiunto alla formazione.

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

**3.1 - Protezione dei dati personali**

La scuola è chiamata ogni giorno a costruire le condizioni per un futuro migliore delle nuove generazioni. Questa sfida riguarda anche il “corretto trattamento dei dati personali”, presupposto necessario per il rispetto della dignità delle persone, della loro identità e del loro diritto alla riservatezza. Pertanto il nostro istituto, durante lo svolgimento dei suoi compiti e rispettando la privacy, si impegna a tutelare i dati personali che si trovano a trattare, visto che i soggetti coinvolti sono minorenni. La protezione dei dati personali è, infatti, 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). Inoltre, il nostro Istituto non solo si occuperà di tutelare la privacy degli/lle studenti/esse e delle loro famiglie, ma anche quello di informare e soprattutto rendere consapevoli gli/le studenti/esse di quanto sia importante tutelare il diritto alla riservatezza di se stessi e degli altri.

**3.2 - Accesso ad Internet**

Per garantire che Internet sia uno strumento finalizzato ai soli scopi formativi saranno implementati sistemi di filtraggio e di identificazione di contenuti non educativi accessibili on line, certificazioni, blocco di pop-up.

I computer fissi presenti nelle aule e nei laboratori accedono ad Internet attraverso rete LAN. I portatili collocati nelle aule accedono tramite wi-fi. I docenti possono accedere con i loro dispositivi personali alla rete wi-fi. Gli studenti possono accedere ad Internet in occasione di attività didattiche che si svolgono nel laboratorio informatico.

La maggior parte delle aule del nostro Istituto sono dotate di un computer collegato alla LIM; alcuni richiedono l'inserimento di una password. Ogni docente è tenuto ad un controllo della strumentazione in aula, poiché l'uso del dispositivo non è permesso agli alunni. I computer si collegano alla rete tramite wi-fi protetta da password e nota al personale docente.

**3.3 - Strumenti di comunicazione online**

Il nostro Istituto, per favorire la digitalizzazione di tutti i reparti scolastici, è dotato di un account di posta elettronica istituzionale, utilizzato ordinariamente dagli uffici amministrativi, e di indirizzi di posta elettronica dei singoli plessi. La posta elettronica è protetta da antivirus e quella certificata anche dall'antispam.

Il nuovo sito web della scuola è gestito dalla Segreteria, da un docente referente e dall'Animatore digitale. Il registro elettronico “Nuvola” è direttamente collegato al sito web e per questo è facilmente fruibile da tutti il personale scolastico e dalle famiglie, alle quali è dedicata un’apposita sezione per le comunicazioni.

**3.4 - Strumentazione personale**

**Per gli studenti: gestione degli strumenti personali - cellulari, tablet ecc.**

Per gli studenti c'è il divieto di utilizzare smartphone e smartwatch per tutte le ore scolastiche. È consentito agli alunni in difficoltà, con DSA e BES, di utilizzare il proprio tablet o notebook con il controllo del docente.

**Per i docenti: gestione degli strumenti personali - cellulari, tablet ecc.**

Durante le ore delle lezioni è consentito l'utilizzo del cellulare solo per attività di servizio, mentre è consentito l'uso di altri dispositivi elettronici personali solo a scopo didattico ed integrativo di quelli scolastici disponibili.

**Capitolo 4 - Rischi online: conoscere, prevenire e rilevare**

**4.1 - Sensibilizzazione e Prevenzione**

Il primo passo che la nostra scuola intende intraprendere è quello del coinvolgimento della comunità scolastica in percorsi di sensibilizzazione e di prevenzione dei comportamenti legati al rischio online.

La diffusione delle tecnologie digitali e dell’accesso alla Rete già nei primissimi anni di vita sta portando profondi cambiamenti nelle dinamiche relazionali e in quelle identitarie, trasformando linguaggi, modalità di comunicazione, abitudini e stili di vita e offrendo inedite potenzialità di crescita.

Una corretta ed efficace sensibilizzazione è necessaria per accrescere la consapevolezza nel gruppo target di riferimento circa un determinato tema/bisogno/problema che potrebbe presentarsi in quel gruppo, incoraggiare il gruppo a modificare i propri comportamenti rendendoli più funzionali, diffondere all’esterno del gruppo di riferimento e quindi tra l’opinione pubblica una certa consapevolezza rispetto all’argomento di interesse, facilitare il coinvolgimento di soggetti esterni in modo da mettere insieme diverse idee per lavorare ad un obiettivo comune.

La sensibilizzazione può costituire il primo passo verso un cambiamento positivo, ma per far sì che l’intervento sia efficace, è importante che sia chiara l’azione verso cui i soggetti devono impegnarsi. Due sono gli aspetti che bisogna tenere in considerazione: la consapevolezza dello status quo; la motivazione al cambiamento.

 È opportuno che i docenti, nell'espletamento delle proprie funzioni di formatori ed educatori, sappiano cogliere ogni opportunità per riflettere insieme agli alunni sui tali rischi.

Fondamentale è monitorare costantemente le relazioni interne alla classe, onde individuare possibili situazioni di disagio ed intervenire tempestivamente, anche mediante il ricorso alle figure di sistema specializzate, per sostenere il singolo nelle situazioni di difficoltà personale e indirizzare il gruppo verso l'instaurazione di un clima positivo, di reciproca accettazione e rispetto, nelle situazioni di difficoltà socio-relazionale.

Tale percorso interno potrà essere ulteriormente rinforzato dalla partecipazione a progetti e/o iniziative esterne coerenti con i temi sopra menzionati, cui la scuola porrà particolare attenzione, selezionando iniziative significative promosse da Enti e/o Associazioni di comprovata affidabilità.

Tra i principali rischi dell'uso delle TIC ricordiamo:

-possibile esposizione a contenuti violenti e non adatti all’età;

- videogiochi diseducativi;

-pubblicità ingannevoli;

-accesso ad informazioni scorrette;

-virus informatici in grado di infettare computer e cellulari;

-possibili contatti con adulti che vogliono conoscere e avvicinare bambini/e o ragazzi/e, e adescamento on-line (grooming);

-rischio di molestie o maltrattamenti da coetanei (cyberbullismo);

-scambio di materiale a sfondo sessuale (sexting);

-uso eccessivo di Internet/cellulare (dipendenza).

È importante conoscere questi fenomeni e saperli distinguere tra loro in modo da poter poi adottare le strategie migliori per poterli arginare e contenere, 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/le ragazzi/e 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.

Parlando di prevenzione in ambito digitale, si potrebbe tradurre quanto appena detto con 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.

Il modello diviso in tre livelli di prevenzione (sotto esplicitato) può essere un’utile guida per affrontare e prevenire ogni possibile situazione di disagio, è tuttavia comprensibile la difficoltà di poter strutturare soluzioni ed interventi multilivello da parte dell’Istituzione Scolastica senza il supporto di altri attori:

-**Prevenzione Universale**. Un programma di questo tipo parte dal presupposto che tutti gli studenti siano potenzialmente a rischio. Si tratta quindi di interventi diretti al grande pubblico o a un intero gruppo di una comunità come quella scolastica che non è stato identificato sulla base del rischio individuale. Efficacia: trattandosi di programmi ad ampio raggio gli effetti di questi programmi possono essere modesti se confrontati con programmi che “trattano” un gruppo con un problema specifico. Tuttavia, questi interventi possono produrre cambiamenti in grandi gruppi (ad es. si pensi ad un programma dedicato alle competenze emotive, oppure alla cittadinanza digitale);

-**Prevenzione Selettiva**. Un programma dedicato ad un gruppo di studenti in cui il rischio online è presente. In questo caso la presenza del rischio viene individuata tramite precedenti indagini, segnalazioni fatte dalla scuola, oppure dalla conoscenza della presenza di fattori di rischio. In questi casi gli interventi sono mirati e prevedono programmi formativi strutturati che hanno l’obiettivo di migliorare le competenze digitali e le strategie di problem solving. Può essere un valido programma se si osservano casi in cui la prevenzione universale non ha dato gli esiti previsti;

-**Prevenzione Indicata**. Un programma di intervento sul caso specifico è quindi pensato e strutturato per adattarsi agli/alle studenti/studentesse con l’obiettivo di ridurre i comportamenti problematici oppure dare supporto alle vittime. Per la sua natura questo tipo di intervento si avvale di professionalità diverse perché spesso affronta problemi legati alla salute mentale del minore per cui è opportuno coinvolgere anche la famiglia del/la ragazzo/a.

I programmi che possono essere realizzati con maggiore frequenza ricadono nel primo livello di Prevenzione Universale e sono sicuramente consigliati proprio perché vanno a formare e consolidare quelle competenze educative di base necessarie a poter gestire le situazioni di vita che i/le ragazzi/e sperimentano online. Per questo motivo la scuola dovrà rafforzare la sua capacità di rispondere anche a questi bisogni attraverso strumenti e misure specifiche. Allo stesso modo quando un evento problematico connesso ai rischi online coinvolge il contesto scolastico, è fondamentale per la scuola poter dare una risposta il più possibile integrata, che trovi la sua espressione di indirizzo in procedure chiare di cui deve dotarsi e che includano la collaborazione (prevedendo accordi specifici) con la rete dei servizi locali (in primis le ASL e la Polizia Postale).

**4.2 – Bullismo e Cyberbullismo: che cos’è e come prevenirlo**

Il BULLISMO (mobbing in età evolutiva) è una forma di comportamento sociale di tipo violento e intenzionale, di natura sia fisica che psicologica, oppressivo e vessatorio, ripetuto nel corso del tempo e attuato nei confronti di persone considerate dal soggetto che perpetra l'atto in questione come bersagli facili e/o incapaci di difendersi. È tipico dell’età pre-adolescenziale e adolescenziale, spesso messo in atto a scuola.

 Gli atti di bullismo si presentano in modi diversi e devono essere distinti chiaramente da quelli che, invece, possono identificarsi come semplici scherzi/giochi inopportuni o ragazzate. Le dimensioni che caratterizzano il fenomeno sono le seguenti:

1.Pianificazione: il bullismo è un comportamento aggressivo pianificato. Il bullo sceglie attentamente la vittima tra i compagni più timidi e isolati per ridurre il rischio di possibili ritorsioni, aspetta che la supervisione dell’adulto sia ridotta e agisce con l’intenzione di nuocere;

2.Potere: il bullo è più forte della vittima, non per forza in termini fisici, ma anche sul piano sociale; il bullo ha un gruppo di amici-complici con cui agisce, mentre la vittima è sola, vulnerabile e incapace di difendersi;

3.Rigidità: i ruoli di bullo e vittima sono rigidamente assegnati;

4.Gruppo: gli atti di bullismo vengono sempre più spesso compiuti da piccole “gang”;

5.Paura: sia la vittima che i compagni che assistono agli episodi di bullismo hanno paura, temono che parlando di questi episodi all’adulto la situazione possa solo peggiorare, andando incontro a possibili ritorsioni da parte del bullo. Meglio subire in silenzio sperando che tutto passi;

 In base a queste dimensioni, il bullismo può assumere forme differenti:

-fisico: atti aggressivi diretti (dare calci, pugni, ecc.), danneggiamento delle cose altrui, furto intenzionale;

-verbale: manifesto (deridere, umiliare, svalutare, criticare, accusare, ecc.) o nascosto (diffondere voci false e offensive su un compagno, provocazioni, ecc.);

-relazionale: sociale (escludere il compagno dalle attività di gruppo, ecc.) o manipolativo (rompere i rapporti di amicizia di cui gode la vittima).

Il CYBERBULLISMO è la manifestazione in rete del fenomeno del bullismo perpetrato soprattutto attraverso i social network, con la diffusione di messaggi offensivi, foto e immagini denigratorie o tramite la creazione di gruppi contro.

Gli alunni di oggi hanno ottime competenze tecniche ma allo stesso tempo mancano ancora di pensiero riflessivo e critico sull’uso delle tecnologie digitali e di consapevolezza sui rischi del mondo digitale. Il confine tra uso improprio e uso intenzionalmente malevolo della tecnologia, tra incompetenza e premeditazione, è sottile. In questo quadro, lo spazio online può diventare un luogo dove il bullismo inizia o è mantenuto.

 A differenza del bullo tradizionale, nel cyberbullo - che già agisce nell’anonimato - viene a mancare un feedback diretto sugli effetti delle aggressioni perpetrate a causa della mancanza di contatto diretto con la vittima. La tecnologia consente ai bulli, inoltre, di infiltrarsi nelle case e nella vita delle vittime, di materializzarsi in ogni momento, perseguitandole con messaggi, immagini, video offensivi inviati tramite diversi device o pubblicati su siti web tramite Internet.

Il cyberbullismo è un fenomeno molto grave perché in pochissimo tempo le vittime possono vedere la propria reputazione danneggiata in una comunità molto ampia, anche perché i contenuti, una volta pubblicati, possono riapparire a più riprese in luoghi diversi. Spesso i genitori e gli insegnanti ne rimangono a lungo all'oscuro, perché non hanno accesso alla comunicazione in rete degli adolescenti. Pertanto può essere necessario molto tempo prima che un caso venga alla luce.

**RIFERIMENTI NORMATIVI**

 Il bullismo e il cyberbullismo devono essere conosciuti e combattuti da tutti in tutte le forme, così come previsto:

-dagli artt. 3-33-34 della Costituzione Italiana;

-dagli artt. 581-582-594-595-610-612-635 del Codice Penale;

-dagli artt. 2043-2047-2048 Codice Civile;

-dalla Direttiva MIUR n.16 del 5 febbraio 2007 recante “Linee di indirizzo generali ed azioni a livello nazionale per la prevenzione e la lotta al bullismo”;

-dalla direttiva MPI n. 30 del 15 marzo 2007 recante “Linee di indirizzo ed indicazioni in materia di utilizzo di ‘telefoni cellulari’ e di altri dispositivi elettronici durante l’attività didattica, irrogazione di sanzioni disciplinari, dovere di vigilanza e di corresponsabilità dei genitori e dei docenti” e successive modifiche/integrazioni;

-dalla direttiva MPI n. 104 del 30 novembre 2007 recante “Linee di indirizzo e chiarimenti interpretativi ed applicativi in ordine alla normativa vigente posta a tutela della privacy con particolare riferimento all’utilizzo di telefoni cellulari o di altri dispositivi elettronici nelle comunità scolastiche allo scopo di acquisire e/o divulgare immagini, filmati o registrazioni vocali”;

-dalla direttiva MIUR n.1455/06;

-dalle Linee di orientamento per azioni di prevenzione e di contrasto al bullismo e al cyberbullismo (MIUR aprile 2015);

-dal D.P.R. 249/98 e 235/2007 recante “Statuto delle studentesse e degli studenti”;

dalla L. 71/2017 “Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo”.

**AZIONI DI TUTELA**

I genitori e le scuole possono sostenere i bambini e i giovani dando loro i giusti consigli e discutendo con loro su quali conseguenze può avere il loro comportamento in rete e cosa significa il cybermobbing per le vittime. Va inoltre segnalato loro che i bulli sono perseguibili penalmente.

I giovani si possono proteggere dal cyberbullismo trattando i dati privati propri e altrui in modo critico e con la massima sensibilità. Ricercando il proprio nome su Internet (il cosiddetto «egosurfing»), ad esempio, si ottengono informazioni sul contesto in cui appare il proprio nome e sulle immagini pubblicate di sé stessi. Chiunque fornisca indicazioni personali o pubblichi immagini su blog, reti sociali o forum si rende un potenziale bersaglio. Ci si può proteggere mantenendo sempre un comportamento rispettoso (netiquette), evitando di postare dati e informazioni sensibili sul proprio profilo (p. es. foto imbarazzanti o troppo discinte), curare solo amicizie personali e proteggere la sfera privata mediante criteri d'impostazione sicuri.

La tutela della sicurezza dei ragazzi che si connettono al web è per la scuola una priorità. Al fine di individuare strategie di prevenzione e di contrasto al cyberbullismo e favorire opportune azioni educative e pedagogiche, la scuola promuove la conoscenza e la diffusione delle regole basilari della comunicazione e del comportamento sul web, come:

-netiquette, un termine che unisce il vocabolo inglese network (rete) e quello francese étiquette (buona educazione): un insieme di regole informali che disciplinano il buon comportamento di un utente sul web di Internet, specie nel rapportarsi agli altri utenti attraverso risorse come newsgroup, mailing list, forum, blog, reti sociali o email;

-norme di uso corretto dei servizi in rete (ad es. navigare evitando siti web rischiosi; non compromettere il funzionamento della rete e degli apparecchi che la costituiscono con programmi virus, malware, etc. – costruiti appositamente);

-sensibilizzazione alla lettura attenta delle privacy policy, il documento che descrive nella maniera più dettagliata e chiara possibile le modalità di gestione e il trattamento dei dati personali degli utenti e dei visitatori dei siti internet e dei social networks da parte delle aziende stesse;

-costruzione di una propria web-reputation positiva;

-sensibilizzazione sugli effetti psico-fisici del fenomeno dilagante del “vamping” (il restare svegli la notte navigando in rete);

-regolamentazione dell’utilizzo dei telefoni cellulari e di altri dispositivi elettronici a scuola.

 **RESPONSABILITA’ DELLE VARIE FIGURE SCOLASTICHE**

L’Istituto Comprensivo dichiara in maniera chiara e ferma l’inaccettabilità di qualsiasi forma di prepotenza, di violenza, di sopruso, di bullismo e di cyberbullismo. Attraverso i propri regolamenti, il patto di corresponsabilità e le strategie educative mirate a costruire relazioni sociali positive l’Istituto coinvolge l’intera comunità educante nel lavoro di prevenzione dei comportamenti problematici, di miglioramento del clima della scuola e di supporto agli studenti in difficoltà. Per tale motivo:

**IL DIRIGENTE SCOLASTICO:**

-individua attraverso il Collegio dei Docenti un referente per il cyberbullismo;

-coinvolge, nella prevenzione e contrasto al fenomeno del bullismo, tutte le componenti della comunità scolastica, particolarmente quelle che operano nell'area dell'informatica, partendo dall'utilizzo sicuro di Internet a scuola;

-prevede corsi di aggiornamento e formazione in materia di prevenzione dei fenomeni del bullismo e cyberbullismo rivolti al personale docente e Ata;

-promuove sistematicamente azioni di sensibilizzazione dei fenomeni del bullismo e cyberbullismo nel territorio in rete con enti, associazioni, istituzioni locali ed altre scuole, coinvolgendo alunni, docenti, genitori ed esperti;

-prevede azioni culturali ed educative rivolte agli studenti, per acquisire le competenze necessarie all’esercizio di una cittadinanza digitale consapevole;

-predispone sul sito internet della scuola uno spazio riservato al tema del cyberbullismo in cui raccogliere il materiale informativo e di restituzione dell’attività svolta dalla scuola.

 **IL REFERENTE DEL BULLISMO E DEL CYBERBULLISMO:**

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

-coordina le attività di prevenzione ed informazione sulle sanzioni previste e sulle responsabilità di natura civile e penale, anche con eventuale affiancamento di genitori e studenti;

-si rivolge a partner esterni alla scuola, quali servizi sociali e sanitari, aziende del privato sociale, forze di polizia, … per realizzare un progetto di prevenzione;

-cura rapporti di rete fra scuole per eventuali convegni/seminari/corsi e per la giornata mondiale sulla Sicurezza in Internet, la “Safer Internet Day” (SID);

-si attiva per la somministrazione di questionari agli studenti e ai genitori (anche attraverso piattaforme on line e con la collaborazione di enti esterni) finalizzati al monitoraggio che possano fornire una fotografia della situazione e consentire una valutazione oggettiva dell’efficacia degli interventi attuati.

**IL COLLEGIO DEI DOCENTI:**

promuove scelte didattiche ed educative, anche in collaborazione con altre scuole in rete, per la prevenzione del fenomeno.

**IL CONSIGLIO DI CLASSE o di INTERCLASSE:**

-pianifica attività didattiche e/o integrative finalizzate al coinvolgimento attivo e collaborativo degli studenti e all'approfondimento di tematiche che favoriscano la riflessione e la presa di coscienza della necessità dei valori di convivenza civile;

-favorisce un clima collaborativo all'interno della classe e nelle relazioni con le famiglie e propone progetti di educazione alla legalità e alla cittadinanza attiva.

**I DOCENTI:**

-intraprendono azioni congruenti con l’utenza del proprio ordine di scuola, tenuto conto che l’istruzione ha un ruolo fondamentale sia nell’acquisizione e rispetto delle norme relative alla convivenza civile, sia nella trasmissione dei valori legati ad un uso responsabile di internet;

-valorizzano, nell'attività didattica, modalità di lavoro di tipo cooperativo e spazi di riflessioni adeguati al livello di età degli alunni;

-monitorano atteggiamenti considerati sospetti o preoccupanti degli alunni, dandone immediata comunicazione al Dirigente Scolastico;

-si impegnano a rimanere aggiornati sulle tematiche del cyberbullismo, anche attraverso corsi di aggiornamento proposti dalla scuola.

 **I GENITORI:**

-partecipano attivamente alle azioni di formazione/informazione, istituite dalle scuole, sui comportamenti sintomatici del bullismo e del cyberbullismo;

-sono attenti ai comportamenti dei propri figli;

-vigilano sull’uso delle tecnologie da parte dei ragazzi, con particolare attenzione ai tempi, alle modalità, agli atteggiamenti conseguenti (i genitori dovrebbero allertarsi se uno studente, dopo l’uso di internet o del proprio telefonino, mostra stati depressivi/ansiosi o paura);

-conoscono le azioni messe in campo dalla scuola e collaborano secondo le modalità previste dal Patto di corresponsabilità;

-conoscono il Regolamento disciplinare d’Istituto.

 **GLI ALUNNI:**

-imparano le regole basilari, per rispettare gli altri, quando sono connessi alla rete, facendo attenzione alle comunicazioni che inviano.

-sono coinvolti nella progettazione e nella realizzazione delle iniziative scolastiche, al fine di favorire un miglioramento del clima e, dopo opportuna formazione, possono operare come tutor per altri studenti;

-si impegnano a diffondere buone pratiche nel rispetto dei diritti di ogni membro della comunità scolastica ed extrascolastica;

-sono consapevoli che non è loro consentito, durante le attività didattiche o comunque all’interno della scuola, acquisire – mediante smartphone o altri dispositivi elettronici – immagini, filmati o registrazioni vocali, se non per finalità didattiche, previo consenso del docente e che, in ogni caso, non è consentita la loro divulgazione, essendo utilizzabili solo per fini personali di studio e documentazione, nel rispetto del diritto alla riservatezza di tutti;

-sono gli attori principali del benessere della comunità scolastica e sono tenuti pertanto a segnalare agli organi preposti (Dirigente scolastico, referente del bullismo/ cyberbullismo, psicologo della scuola, docenti, etc…) eventuali atti di bullismo e cyberbullismo di cui sono a conoscenza, consapevoli del fatto che verrà garantita loro la riservatezza di quanto comunicato.

**STRUMENTI DI SEGNALAZIONE**

Alunni, famiglie, docenti e tutto il personale scolastico attivo nell’Istituto si impegnano a segnalare al Dirigente Scolastico i casi di bullismo e cyberbullismo di cui sono a conoscenza, anche se presunti, in modo da attivare tutte le procedure di verifica necessarie all’individuazione del bullo, della vittima e delle dinamiche intercorse tra i due.

Si ricorda che la L.71/2017 – Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo – pone molta attenzione ai reati di INGIURIA, DIFFAMAZIONE, MINACCIA e VIOLAZIONE DEI DATI PERSONALI, facendo riferimento agli articoli 594, 595 e 612 del Codice Penale e all’articolo 167 del Codice per la protezione dei dati personali.

**4.3 - Hate speech: che cos’è e come prevenirlo**

ll fenomeno di “incitamento all’odio” o “discorso d’odio”, indica discorsi (post, immagini, commenti…) 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, etc.) ai danni di una persona o di un gruppo. Tale fenomeno, purtroppo, negli ultimi anni si è fortemente diffuso e rafforzato soprattutto attraverso l’uso della Rete, i social network in particolar modo, dove non è difficile e infrequente trovare forme di odio e hate speech online particolarmente violente. Per questo è estremamente importante affrontarlo con ragazze e ragazzi anche a scuola. Tale fenomeno, purtroppo, negli ultimi anni si è fortemente diffuso e rafforzato soprattutto attraverso l’uso della Rete, i social network in particolar modo, dove non è difficile e infrequente trovare forme di odio e hate speech online particolarmente violente. Per questo è estremamente importante affrontarlo con ragazze e ragazzi anche a scuola.

Internet è difficilmente controllabile. La diffusione di messaggi di incitamento all’odio è maggiormente tollerata su Internet rispetto al mondo offline ed è sottoposta a minori controlli. È ugualmente più facile (e comporta meno rischi) insultare o molestare online, perché le persone spesso si esprimono sotto la copertura dell’anonimato. L’impunità e anonimato sono le due presunte caratteristiche delle interazioni sociali in rete. Queste abbassano le remore etiche. In realtà, però, qualsiasi azione compiuta sul web consente di rintracciare il suo autore.

Il discorso dell’odio si manifesta con un ampio spettro di azioni: sebbene tutte le espressioni che istigano all’odio meritino di essere classificate come malvagie, ne esistono alcune che possono essere peggiori di altre. È utile, quindi, prendere in considerazione alcuni aspetti:

- il contenuto e il tono: certe espressioni di odio sono più estreme, utilizzano termini più insultanti e possono perfino istigare altri ad agire. All’altra estremità della scala, troviamo insulti più moderati o generalizzazioni eccessive, che presentano certi gruppi o individui sotto una cattiva (e perfino sotto falsa) luce;

-intenzione degli autori degli insulti: ci può capitare di offendere gli altri senza volerlo, e poi di pentircene, e perfino di ritirare quanto abbiamo detto;

-i bersagli o i bersagli potenziali: alcuni gruppi, o individui, possono essere più vulnerabili di altri alle critiche. Può dipendere dal modo in cui sono globalmente considerati nella società, o da come sono rappresentati nei media, oppure dalla loro situazione personale, che non permette loro di difendersi efficacemente;

-il contesto di una particolare espressione di odio è legato talvolta a circostanze storiche e culturali specifiche. Può includere altri fattori, come il mezzo utilizzato e il gruppo preso di mira, le tensioni o i pregiudizi esistenti, l’autorità del suo autore, etc.- L’impatto reale o potenziale esercitato sugli individui, sui gruppi o sull’insieme della società è una delle principali considerazioni da tenere presenti. Spesso, le ripercussioni negative subite dall’individuo o dal gruppo si rivelano più importanti della valutazione dell’episodio da parte di osservatori esterni.

L’Istituto intende:

-promuovere lo sviluppo delle competenze digitali e l’educazione ad un uso etico e consapevole delle tecnologie assumono quindi un ruolo centrale anche per la promozione della consapevolezza di queste dinamiche in rete;

-in tal senso fornire ai più giovani gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di hate speech;

-promuovere la partecipazione civica e l’impegno, anche attraverso i media digitali e i social network. Nello specifico pensare ad attività di analisi e produzione mediale, finalizzate soprattutto a fornire agli studenti gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di hate speech, in particolare legati alla razza, al genere, all’orientamento sessuale, alla disabilità.

**4.4 - Dipendenza da Internet e gioco online**

La dipendenza da Internet, che può manifestarsi anche attraverso le ore trascorse online a giocare, rappresenta una questione importante per la comunità scolastica che deve attenzionare il fenomeno e fornire gli strumenti agli studenti e alle studentesse affinché questi siano consapevoli dei rischi che comporta l’iperconnessione. Secondo l’Istat, “nel 2018, l’85,8% dei ragazzi tra 11 e 17 anni di età utilizza quotidianamente il telefono cellulare. Il 72% dei ragazzi in quella stessa fascia di età naviga in Internet tutti i giorni. Questa quota è cresciuta molto rapidamente passando dal 56,2 al 72,0% nell’arco di un quadriennio. Le più frequenti utilizzatrici del cellulare e della rete sono le ragazze, l’87,5% delle quali usa il cellulare quotidianamente e il 73,2% accede a Internet tutti i giorni (quota che sale all’84,9% se ci si concentra sulle adolescenti tra i 14 e i 17 anni). Spesso il trascorrere del tempo online, in termini disfunzionali, è scandito dal gioco virtuale che può anche assumere forme di Dipendenza dal gioco online (Net gaming addiction o Internet Gaming Addiction) inserito all’interno del Manuale Diagnostico Statistico dei Disturbi Mentali (DSM 5). Da specificare che la dipendenza qui si realizza quando c’è un abuso, ossia un utilizzo continuativo e sistematico della Rete al fine di giocare impegnando la maggior parte delle giornate, con la conseguente sottrazione del tempo alle altre attività quotidiane del minore.

I segnali patologici di questo che viene descritto come “un vero e proprio abuso della tecnologia”, anche denominato “Internet Addiction Disorder”, sono specifici così come accade per le altre dipendenze più “tradizionali”. In particolare, si ha la tolleranza quando vi è un crescente bisogno di aumentare il tempo su internet e l’astinenza quando vi è l’interruzione o la riduzione dell’uso della Rete che comporta ansia, agitazione psicomotoria, fantasie, pensieri ossessivi (malessere psichico e/o fisico che si manifesta quando s’interrompe o si riduce il comportamento). Tutto questo ha ripercussioni sulla sfera delle relazioni interpersonali che diventano via via più povere e alle quali si preferisce il mondo virtuale, con alterazioni dell’umore e della percezione del tempo.

La scuola può insegnare molto da questo punto di vista se integra la tecnologia nella didattica, mostrando un suo utilizzo funzionale che possa rendere più consapevoli i ragazzi e le ragazze delle proprie abitudini online. Può aiutare nel controllo sulla tecnologia per poterne usare il pieno potenziale e trarne vantaggi, strutturando regole condivise e stipulando con gli alunni una sorta di “patto” d’aula e, infine, proporre delle alternative metodologiche e didattiche valide che abbiano come strumento giochi virtuali d’aula. È importante, quindi, non demonizzare la tecnologia o il gioco, ma cercare di entrare nel mondo degli/lle studenti e delle studentesse, stabilendo chiare e semplici regole di utilizzo.

**4.5 – Sexting**

Il sexting (abbreviazione di sex – sesso e texting – messaggiare, inviare messaggi) indica l’invio e/o la ricezione di contenuti (video o immagini) sessualmente espliciti che ritraggono se stessi o gli altri. Spesso sono realizzate con il telefonino, e vengono diffuse attraverso il cellulare o attraverso siti, e-mail, chat. Spesso tali immagini o video, anche se inviate ad una stretta cerchia di persone, si diffondono in modo incontrollabile e possono creare seri problemi, sia personali che legali, alla persona ritratta. La consapevolezza, o comunque la sola idea di diffusione di contenuti personali, si replica nel tempo e può finire con il danneggiare, sia in termini psicologici che sociali, sia il ragazzo/la ragazza soggetto della foto/del video che colui/coloro che hanno contribuito a diffonderla. Due agiti, quindi, che sono fra loro strettamente legati e che rappresentano veri e propri comportamenti criminali i quali hanno ripercussioni negative sulla vittima in termini di autostima, di credibilità, di reputazione sociale off e on line. A ciò si associano altri comportamenti a rischio, di tipo sessuale ma anche riferibili ad abuso di sostanze o di alcool.

**4.6 - Adescamento online**

I luoghi virtuali in cui si sviluppano più frequentemente le dinamiche di adescamento online 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.

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

L'Istituto per prevenire casi di adescamento online realizzerà un percorso di educazione (anche digitale) all’affettività e alla sessualità per accompagnare ragazze e ragazzi. Ciò per renderli più sicuri emotivamente e pronti ad affrontare eventuali situazioni a rischio, imparando innanzitutto a gestire le proprie emozioni, il rapporto con il proprio corpo e con gli altri. È molto importante, inoltre, che i docenti siano un punto di riferimento per ragazzi e ragazze in modo che quest'ultimi sappiano a chi rivolgersi in caso di problemi, anche quando pensano di aver fatto un errore, si vergognano o si sentono in colpa. Gli adulti coinvolti, genitori e docenti, devono essere supporto costante per il minore che deve potersi fidare di loro e non sentirsi mai giudicato, ma compreso e ascoltato. Affinché ciò avvenga è necessario tenere sempre aperto un canale di comunicazione con loro sui temi dell’affettività, del digitale e perché no, della sessualità.

Il nostro Istituto in caso di adescamento online richiederà l’intervento della Polizia Postale e delle Comunicazioni a cui bisogna rivolgersi il prima possibile, tenendo traccia degli scambi fra il minore e l’adescatore (ad esempio, salvando le conversazioni attraverso screenshot, memorizzando eventuali immagini o video…).

L’adescamento, inoltre, può essere una problematica molto delicata da gestire e può avere ripercussioni psicologiche significative sul minore. Per questo potrebbe essere necessario rivolgersi ad un Servizio territoriale (es. Consultorio Familiare, Servizio di Neuropsichiatria Infantile, ecc.) in grado di fornire alla vittima anche un adeguato supporto di tipo psicologico o psichiatrico.

**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 coinvolte/i in comportamenti sessualmente espliciti, concrete o simulate o qualsiasi rappresentazione degli organi sessuali a fini soprattutto sessuali. La pedopornografia esiste da prima dell’avvento di Internet. Tuttavia, la diffusione della Rete, l’evoluzione e la moltiplicazione dei “luoghi” virtuali, il cambiamento costante delle stesse tecnologie digitali, ha radicalmente cambiato il modo in cui il materiale pedopornografico viene prodotto e diffuso, contribuendo ad un aumento della sua disponibilità e dei canali di diffusione. La diffusione della banda larga, ad esempio, consente di caricare e scaricare velocemente video e foto anche di grandi dimensioni, così come la diffusione delle videocamere e dei cellulari con videocamera incorporata, consente la produzione “in house” di materiale video, riproducibile facilmente online.

Se si ravvisa un rischio per il benessere psicofisico dei/lle bambini/e, ragazzi/e coinvolte nella visione di questi contenuti si ricorrerà a un supporto psicologico anche passando per una consultazione presso il medico di base o pediatra di riferimento. Le strutture pubbliche a cui rivolgersi sono i servizi socio-sanitari del territorio di appartenenza: Consultori Familiari, Servizi di Neuropsichiatria infantile, centri specializzati sull’abuso e il maltrattamento all’infanzia, etc.

L'Istituto organizzerà attività educativa sull’affettività e le relazioni, sottolineando sempre la necessità di rivolgersi ad un adulto quando qualcosa online mette a disagio.

Inoltre, si adopererà per l'organizzazione di un’attività di sensibilizzazione rivolta ai genitori e al personale scolastico.