Documento di ePolicy

BSIS00600C

ISTITUTO ISTRUZIONE SUPERIORE C.BERETTA

VIA G. MATTEOTTI 299 - 25063 - GARDONE VAL TROMPIA - BRESCIA (BS)

Stefano Retali

Capitolo 1 - Introduzione al documento di ePolicy

1.1 - Scopo dell'ePolicy

Le TIC (Tecnologie dell'informazione e della comunicazione) rappresentano strumenti fondamentali nel processo educativo e per l'apprendimento degli studenti e delle studentesse.

Le "competenze digitali" sono fra le abilità chiave all'interno del Quadro di riferimento Europeo delle Competenze per l'apprendimento permanente e di esse bisogna dotarsi proprio a partire dalla scuola (Raccomandazione del Consiglio Europeo del 2006 aggiornata al 22 maggio 2018, relativa alle competenze chiave per l'apprendimento permanente).

In un contesto sempre più complesso, diventa quindi essenziale per ogni Istituto Scolastico dotarsi di una E-policy, un documento programmatico volto a promuovere le competenze digitali ed un uso delle tecnologie positivo, critico e consapevole, sia da parte dei ragazzi e delle ragazze che degli adulti coinvolti nel processo educativo. L'E-policy, inoltre, vuole essere un documento finalizzato a prevenire situazioni problematiche e a riconoscere, gestire, segnalare e monitorare episodi legati ad un utilizzo scorretto degli strumenti.

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

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

Argomenti del Documento

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

5. Gestione delle infrazioni alla ePolicy
6. Integrazione dell'ePolicy con regolamenti esistenti
7. Monitoraggio dell'implementazione dell'ePolicy e suo aggiornamento

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

Perché è importante dotarsi di una E-policy?

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

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

1.2 - Ruoli e responsabilità

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

IL DIRIGENTE SCOLASTICO

è garante per la sicurezza di tutti i membri della comunità scolastica e come tale:

- deve essere adeguatamente formato sulla sicurezza e prevenzione di problematiche offline e online, in linea con le leggi di riferimento e i suggerimenti del MIUR e delle sue agenzie;
- deve promuovere la cultura della sicurezza online integrandola ed inserendola nelle misure di sicurezza più generali dell'intero Istituto;
- ha la responsabilità di fornire sistemi per un uso sicuro delle TIC, internet, suoi strumenti ed ambienti;
- ha la responsabilità della gestione dei dati e della sicurezza delle informazioni e garantisce che l'Istituto segue le pratiche migliori possibili nella gestione dei dati stessi.
- deve tutelare la scuola e garantire agli utenti la sicurezza di navigazione utilizzando adeguati sistemi informatici e servizi di filtri Internet;
- ha il compito di garantire a tutto il personale una formazione adeguata sulla sicurezza online per essere tutelato nell'esercizio del proprio ruolo educativo e non;
- deve essere a conoscenza delle procedure da seguire in caso di un grave incidente di sicurezza online;
- deve garantire adeguate valutazioni di rischio nell'usare strumenti e TIC, effettuate in modo che comunque quanto programmato possa soddisfare le istanze educative e didattiche dichiarate nel PTOF di Istituto;
- deve garantire l'esistenza di un sistema che assicuri il monitoraggio e il controllo interno della sicurezza on- line in collaborazione con le figure di sistema;
- deve essere a conoscenza ed attuare le procedure necessarie in caso di grave incidente di sicurezza online;

- assicura che sito web della scuola includa informazioni sulla cultura della sicurezza online, rilevanti e condivise con i diversi stakeholders;

- deve ricevere le relazioni periodiche dello stato di sicurezza della rete da parte dal Referente.

Il RESPONSABILE DELLA SICUREZZA ONLINE e la DSGA , che ha responsabilità nei confronti del personale amministrativo incaricato al trattamento dei dati:

- assicurano, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per garantire che l'infrastruttura tecnica della scuola sia funzionante, sicura e non aperta a uso improprio o a dannosi attacchi esterni;

- assicurano che gli utenti possano accedere alla rete della scuola solo tramite password personali applicate e regolarmente cambiate e curare la manutenzione e lo sviluppo del sito web della scuola per scopi istituzionali e consentiti (istruzione e formazione);

- garantiscono il funzionamento dei diversi canali di comunicazione all'interno dell'Istituto (registro classe viva Spaggiari,sito web, ecc.) e fra la scuola e le famiglie degli alunni per la notifica di documenti e informazioni del Dirigente scolastico e dell'Animatore digitale nell'ambito dell'utilizzo delle tecnologie digitali e di internet;

- promuovono la consapevolezza e l'impegno per la salvaguardia online in tutta la comunità scolastica;

- garantiscono che tutto il personale sia a conoscenza delle procedure che devono essere seguite in caso di incidente per la sicurezza online;

- coordinano i vari interventi con le autorità locali e le agenzie competenti;

- garantiscono che tutti i dati relativi agli alunni pubblicati sul sito siano sufficientemente tutelati.

L'ANIMATORE DIGITALE e I REFERENTI DEL BULLISMO E CYBERBULLISMO

L'ANIMATORE DIGITALE

- stimola la formazione interna all'istituzione negli ambiti di sviluppo della "scuola digitale" e fornisce consulenza e informazioni al personale in relazione ai rischi on-line;

- coinvolge la comunità scolastica (alunni, genitori e altri attori del territorio) nella partecipazione ad attività e progetti attinenti la “scuola digitale”;
- rileva le problematiche emergenti relative all’utilizzo delle tecnologie digitali e di internet nonché propone la revisione delle politiche dell’istituzione con l’individuazione di soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola.

I REFERENTI DEL BULLISMO E CYBERBULLISMO

- promuovono e o coordinano iniziative di prevenzione e contrasto del cyberbullismo messe in atto dall’Istituto;
- facilitano la formazione e la consulenza di tutto il personale e degli alunni sulle tematiche di propria competenza.

I DOCENTI

- provvedono alla formazione/aggiornamento sull’utilizzo e l'integrazione delle TIC nella didattica, sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali; e sulla Gestione dell'infrastruttura e della strumentazione ICT della scuola;
- inseriscono tematiche legate alla sicurezza online nelle programmazioni didattiche eventualmente trasversali;
- supportano gli alunni nell’utilizzo consapevole delle tecnologie informatiche utilizzate a scopi didattici;
- segnalano al Dirigente Scolastico e ai suoi collaboratori eventuali episodi di violazione delle norme dicomportamento stabilite dalla scuola, avviando le procedure previste in caso di violazione;
- rispettano l’obbligo di riservatezza dei dati personali trattati e non, in conformità alla normativa vigente;
- interagiscono con i genitori, coordinando con gli stessi l’intervento educativo, nei casi di disagio, manifestato dall’alunno, collegato all’utilizzo delle tecnologie digitali;
- segnalano all’Animatore digitale eventuali criticità nei sistemi informativi soprattutto in materia di prevenzione e gestione dei rischi nell’uso delle TIC;

- condivideono con gli alunni le competenze in uscita degli stessi;
- supervisionano e guidano gli alunni con cura quando sono impegnati in attività di apprendimento con la tecnologie online;
- responsabilizzano gli alunni relativamente ai problemi legali dei contenuti elettronici come ad esempio siti illegali, plagio, leggi sul copyright;
- responsabilizzano e fanno conoscere il regolamento relativo al corretto utilizzo a scuola dei dispositivi elettronici: cellulari, fotocamere, dispositivi portatili e i relativi problemi di sicurezza online;
- mantengono tutte le comunicazioni digitali con alunne/alunni e genitori/tutori a livello professionale e realizzarle esclusivamente con sistemi ufficiali scolastici.

GLI ALUNNI

- leggono, comprendono e accettano la E – Safety Policy;
- conoscono e applicano le regole per il corretto utilizzo dei dispositivi elettronici/multimediali a scuola;
- informano immediatamente il docente di qualsiasi 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;
- evitano il plagio, rispettare le normative sul diritto d'autore, non diffondere dati personali;
- capiscono le politiche di utilizzo delle immagini ed essere consapevoli del significato e della gravità del cyberbullismo;
- non inviano materiali abusivi, offensivi o inappropriati durante le attività didattiche;
- rispettano il divieto di ripresa non permessa di eventi, fatti e situazioni durante le attività didattiche.

I GENITORI

- accettano la E – Safety Policy e sostenere i docenti nell'azione educativa diretta alla promozione della sicurezza online ;
- leggono, comprendono e controfirmanno il presente accordo inserito nel Patto Educativo di Corresponsabilità;
- educano (vigilando sui propri figli) al corretto utilizzo delle tecnologie digitali in ambiente domestico fissando regole comportamentali e di utilizzo;
- conoscono il Regolamento d'Istituto e i relativi provvedimenti disciplinari da applicare in caso di violazione delle disposizioni.

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).

In relazione a ciò, nel nostro istituto, tutti gli enti educativi esterni e le associazioni e in genere tutti i soggetti esterni di qualunque natura che entrano in relazione con la scuola devono conformarsi alla

politica della stessa riguardo all'uso consapevole della rete e delle TIC; inoltre, devono promuovere la sicurezza online e assicurare la protezione degli studenti e delle studentesse durante le attività.

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.

Inoltre i docenti, gli studenti, le famiglie condividono nella nostra comunità scolastica i seguenti aspetti.

CORPO DOCENTE

I. Approvazione a livello collegiale;

II. confronto collegiale, su base annuale, circa la necessità di apportare modifiche e miglioramenti alla policy vigente;

III. elaborazione di protocolli condivisi di intervento.

COMPONENTE STUDENTESCA

I. Conoscenza del documento "Policy" nei primi giorni di scuola, da inserire anche nel progetto di accoglienza per le nuove classi prime;

GENITORI

I.Eventuale organizzazione di incontri di sensibilizzazione sul tema della sicurezza informatica;

II. informazione e formazione circa i comportamenti da monitorare e/o da evitare; gli adulti hanno un ruolo fondamentale nel garantire che gli studenti siano in grado di utilizzare le tecnologie digitali e che lo facciano in modo appropriato e sicuro, e questo coinvolge a pieno titolo tutti gli educatori e i formatori, primi fra tutti i genitori e la comunità scolastica nel suo complesso. Non va tuttavia sottovalutato il ruolo degli studenti come primi attori del percorso di acquisizione della capacità di positiva gestione delle proprie competenze digitali. In tale ottica si rende indispensabile coinvolgere anche i più giovani, non solo quali destinatari, ma anche interlocutori attivi e propositivi di tutte le azioni e gli interventi volti alla piena attuazione della Policy.

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.

Tutte le infrazioni alla presente Policy andranno tempestivamente segnalate al Dirigente Scolastico, che avrà cura di convocare le parti interessate onde valutare le possibili azioni da intraprendere. E' fondamentale per l'Istituto, anche nella sanzione, creare sempre occasioni di recupero. Da ciò discende quanto segue.

• La Scuola prenderà e manterrà nel tempo tutte le precauzioni necessarie e adatte per garantire agli studenti l'accesso a materiale e ambienti appropriati.

• Il Referente per il bullismo e/o il referente e-safety e il suo team sono coloro ai quali bisogna rivolgersi immediatamente nel caso in cui si verifichino incidenti o comportamenti dubbi.

• Qualsiasi sospetto, rischio, violazione va segnalato in giornata ai suddetti Referenti che riferiscono al Dirigente.

• Al personale, agli studenti e agli altri componenti della comunità scolastica sono date informazioni sulle infrazioni previste e le eventuali sanzioni.

• Le sanzioni riferite soprattutto agli alunni avranno come carattere preferenziale quello educativo/riabilitativo e in ogni caso verrà coinvolta la componente genitori, in qualità di primi educatori.

• All'interno del Regolamento d'Istituto si trovano invece le diverse sanzioni, graduate in modo proporzionale rispetto alla gravità delle varie forme di bullismo (art. 4 DPR 249 del 1998). 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 quelli riportati di seguito.

1. Minaccia, in particolare, se la minaccia è grave, per tale reato si procede d'ufficio (art. 612 codice penale);
2. Induzione alla prostituzione minorile (art. 600bis);
3. Pedopornografia (art. 600ter);
4. Corruzione di minorenne (art. 609quinquies).

Nel caso in cui le infrazioni della policy 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.

Questo documento in tutte le sue parti viene prodotto in modo da integrare per finalità, obiettivi e contenuti con i documenti che specificano le politiche dell'Istituto per un uso efficace e consapevole del digitale nella didattica:

- PTOF;

- Regolamento d'istituto con relativa integrazione sul bullismo e cyberbullismo;

- Patto educativo di Corresponsabilità e relativa integrazione.

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.

Inoltre potranno essere necessarie integrazioni o modificazioni della nostra policy in relazione a norme di maggior valore come regolamenti o Policy emanati dal MIUR o eventuali leggi dello Stato, ovvero ogni eventuale aggiornamento avverrà anche sulla base di casi problematici riscontrati.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica

- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i docenti dell'Istituto per la stesura finale dell'ePolicy.
- Organizzare incontri per la consultazione degli studenti/studentesse sui temi dell'ePolicy per cui si evidenzia la necessità di regolamentare azioni e comportamenti.
- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i genitori dell'Istituto per la stesura finale dell'ePolicy.
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto agli studenti.
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai docenti.
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai genitori.
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto agli studenti.
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai docenti.

- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai genitori.

Azioni da svolgere nei prossimi 3 anni

- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i docenti dell'Istituto per la stesura finale dell'ePolicy.
- Organizzare incontri per la consultazione degli studenti/studentesse sui temi dell'ePolicy per cui si evidenzia la necessità di regolamentare azioni e comportamenti.
- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i genitori dell'Istituto per la stesura finale dell'ePolicy.
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto agli studenti.
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai docenti.
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai genitori.
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto agli studenti.
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai docenti.
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai genitori.

Capitolo 2 - Formazione e curricolo

2.1. Curricolo sulle competenze digitali per gli studenti

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

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

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

I nostri alunni debbono essere messi nelle condizioni di comprendere, imparare ed utilizzare le TIC in modo responsabile . Tutto ciò al fine di scambiare, esplorare navigando, cercare e presentare informazioni in modo il più responsabile possibile ed essere in grado di avere un rapido accesso a idee ed esperienze provenienti da persone, comunità e culture diverse molto presenti nelle realtà dei nostri tre plessi. A noi spetta quindi anche il compito di trovare raccordi efficaci tra la crescente dimestichezza degli alunni con le Tecnologie dell'Informazione e della Comunicazione e l'azione didattica quotidiana. Si rende quindi necessario lo sviluppo e la diffusione di una mentalità tecnologica diffusa e precoce, come forma di alfabetizzazione all'utilizzabilità in contesti dati e per scopi definiti da un lato; ed acquisizione sempre più consapevole di strategie efficaci per il dominio di una macchina complessa che impiega e genera oggetti immateriali, dall'altro.

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.

Nel nostro istituto sono presenti un gruppo consistente di insegnanti con forti competenze informatiche mentre altri iniziano a conoscere questo mondo anche grazie a corsi di formazione mirati ad acquisire queste conoscenze e competenze. La dirigenza promuove la partecipazione del personale ad iniziative istituite sia direttamente dalla scuola attraverso il piano annuale per la formazione dei docenti, sia dalle reti di scuole e dall'amministrazione, sia quelle liberamente scelte dai docenti (anche online), purché coerenti con il piano di formazione. La formazione del corpo docente è organizzata su due livelli: interno ed esterno. A livello interno, il PTOF prevede che una parte della formazione in servizio, obbligatoria ai sensi della L. 107/2015, sia dedicata proprio all'uso e all'inserimento delle TIC nella didattica e ai temi informatici in generale. Tale formazione potrà essere svolta da docenti dell'Istituto che fanno parte del team per l'innovazione digitale. Il percorso formativo concordato collegialmente sarà finalizzato alla condivisione di esperienze significative e di buone pratiche nell'ottica di migliorare la professionalità dei docenti, uno degli obiettivi da raggiungere. Per quanto riguarda la formazione esterna, la scuola assicurerà una tempestiva e capillare informazione su corsi della Rete di Ambito 6, convegni e seminari che riguardino tali argomenti, agevolando il personale che intenda parteciparvi. I risultati di questi percorsi formativi consentono alla maggior parte dei docenti di acquisire buone competenze digitali spendibili per una didattica innovativa, per il successo scolastico e formativo e per l'inclusione di tutti gli alunni.

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

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

amministrazioni comunali, dei servizi socio-educativi e delle associazioni presenti.

La formazione specifica dei docenti sull'utilizzo consapevole e sicuro di Internet, include importanti esperienze, infatti alcuni docenti aderiscono anche, tra le altre, alla formazione on line sulla piattaforma "Generazioni Connesse", che offre numerosi materiali informativi sia per l'approfondimento personale che per le attività da proporre agli alunni.

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.

Infatti, come dalle "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del "cyberbullismo", si prevedono l'integrazione, oltre che del Regolamento scolastico, anche del "Patto di Corresponsabilità", con specifici riferimenti a condotte di cyberbullismo e i policy e relative sanzioni disciplinari "commisurate alla gravità degli atti compiuti", al fine di meglio regolamentare l'insieme dei provvedimenti sia di natura disciplinare che di natura educativa e di prevenzione al fenomeno.

Il nostro piano d'azioni

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

Scegliere almeno 1 di queste 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.
- Organizzare e promuovere per il corpo docente incontri formativi sull’utilizzo e l’integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi sull’utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare incontri con esperti per i docenti sulle competenze digitali.
- Organizzare incontri con esperti per i genitori sull’educazione alla cittadinanza digitale.

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

Scegliere almeno 1 di queste 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.

- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare incontri con esperti per i docenti sulle competenze digitali.
- Organizzare incontri con esperti per i genitori sull'educazione alla cittadinanza digitale.

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

3.1 - Protezione dei dati personali

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

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

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

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

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

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

personali.

Si fa riferimento a tutto quanto previsto dal Decreto legislativo 30 giugno 2003, n. 196 (c. d. Codice della Privacy) e dal nuovo Regolamento europeo Privacy. Tuttavia si possono individuare al riguardo alcune linee guida di e-safety.

Il personale condivide ad esempio quanto riportato di seguito.

- Numeri di telefono personali o indirizzi di posta elettronica privati con la componente studentesca e con i genitori solo per scopi didattici.
- All'atto dell'iscrizione è richiesto alle famiglie di firmare un'autorizzazione scritta per consentire l'uso didattico, con eventuale pubblicazione sul sito scolastico, di immagini, video e nominativi con finalità istituzionali.
- Eventuali fotografie o video, che includano allieve e allievi in occasione di eventi di particolare evidenza pubblica gestiti da terzi, verrà espressamente richiesta alle famiglie una liberatoria specifica.
- Ogni ulteriore caso particolare sarà preso in considerazione per stabilire l'opportunità di pubblicare dati personali e sarà presentata apposita richiesta circostanziata che varrà solo per lo specifico evento.

Il titolare del trattamento dei dati personali è l' IIS "BERETTA" rappresentato dal Dirigente Scolastico.

Il Responsabile per la Protezione dei Dati è rappresentato da soggetto esterno.

- Il titolare effettua il trattamento di un’ampia categoria di dati personali, compresi quelli appartenenti a categorie particolari.

- Il trattamento dei dati per conto del Titolare è effettuato sia dai dipendenti e dai collaboratori del Titolare, nella loro qualità di incaricati e/o amministratori di sistema, di docenti, sia del personale di soggetti esterni, nella loro qualità di responsabili del trattamento.

In tutti i casi sono rispettati i principi alla base del corretto trattamento dei dati; gli incaricati sono formati e i responsabili del trattamento nominati e sensibilizzati al rispetto dei dettami del Regolamento, nel rispetto del principio di stretta indispensabilità dei trattamenti.

Misure operative specifiche all’utilizzo di tecnologie informatiche:

- scegliere per i diversi software gestionali (area Personale, area Didatca, eccetera) una password che sia composta da caratteri non facilmente intuibile, evitando che contenga riferimenti alla propria persona (es. proprio nome o di congiunti, date di nascita, ecc.);
- curare la conservazione della propria password dei software gestionali e non comunicarla per alcun motivo a sogget terzi;
- cambiare periodicamente (almeno una volta ogni tre mesi) la propria password dei software gestionali;
- adottare le stesse cautele di cui sopra per le password di qualsiasi altra piattaforma software ad uso personale e potenzialmente interessata al Trattamento di Dati Personali (mail,

account per piattaforme terze, eccetera);
- effettuare il logoff dai software gestionali e, laddove presenti, da sistemi di autenticazione di rete al termine di ogni sessione di lavoro;
- spegnere correttamente il computer al termine di ogni sessione di lavoro al fine di agevolare, se utilizzati, l'azione di software specifici di congelamento delle configurazioni degli stessi;
- non abbandonare la propria postazione di lavoro per la pausa o altri motivi senza aver spento la postazione di lavoro o aver inserito uno screen saver con password;
- nella comunicazione multimediale con alunni e genitori utilizzare esclusivamente le piattaforme informatiche messe a disposizione dall'Istituto; è fatto divieto utilizzare social network quali Facebook o altri che non abbiano carattere istituzionale;
- nell'utilizzo della posta elettronica non aprire documenti di cui non sia certa la provenienza e controllare accuratamente l'indirizzo dei destinatari prima di inviare email contenenti in allegato o nel corpo del messaggio dati personali;
- nell'esercizio delle proprie mansioni utilizzare esclusivamente le apparecchiature informatiche fornite dalla scuola, presenti negli uffici di segreteria: ufficio segreteria del personale, ufficio di segreteria didattica, ufficio affari generali, in quanto tali attrezzature sono regolarmente sottoposte a rigide misure di sicurezza e in linea con le misure minime di sicurezza ICT emanate dall'AGID.

3.2 - Accesso ad Internet

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

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

Il diritto di accesso a Internet è dunque presente nell'ordinamento italiano ed europeo e la scuola dovrebbe essere il luogo dove tale diritto è garantito, anche per quegli studenti che non dispongono della Rete a casa. In modo coerente il PNSD (Piano Nazionale Scuola Digitale) ha tra gli obiettivi quello di "fornire a tutte le scuole le condizioni per l'accesso alla società dell'informazione e fare in modo che il "diritto a Internet" diventi una realtà, a partire dalla scuola".

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

L'Istituto attualmente è dotato di una rete wireless destinata all'utilizzo da parte del corpo docente e degli alunni in un'ottica di didattica. La scuola assegna una password per ciascun utente allo scopo di impedire e monitorare meglio eventuali usi impropri. In particolare l'IIS "Beretta" intende mantenere un log corrente sull'uso dei sistemi della scuola per la verifica di eventuali violazioni della policy, oltre che delle leggi vigenti, da parte di chiunque abbia accesso a essi.

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;
- rispettare la cosiddetta "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 email).

I genitori saranno invitati a firmare e restituire un modulo di consenso.

La componente studentesca dovrà impegnarsi a rispettare le norme di buon utilizzo che la scuola si impegna a redigere e a divulgare prima che sia concesso l'accesso a Internet.

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.

L'Istituto" Beretta "utilizza il registro elettronico "Classe Viva Spaggiari", sfruttandone al meglio tutte le potenzialità connesse, ciò permette di rendere immediate, trasparenti ed efficaci le

comunicazioni all'interno della scuola e fra scuola e famiglie.

Ogni famiglia riceve le credenziali, distintamente genitori ed alunni, per l'accesso riservato al registro elettronico, in cui il corpo docente è tenuto a registrare assenze, valutazioni, note e osservazioni.

Le famiglie che non possono accedere temporaneamente a Internet e di conseguenza non possono consultare il registro elettronico devono avvisare la segreteria didattica che provvederà in proposito.

I dati di contatto sul sito web sono: indirizzo della scuola, e-mail istituzionale e numero di telefono.

Il sito prevede un'area pubblica per le informazioni che non comportano la diffusione di dati personali o riservati, in cui sono reperibili le informazioni sulla vita scolastica, iniziative e scadenze ministeriali, avvisi di carattere generale, e un'area riservata accessibile solo dopo autenticazione. Il Dirigente Scolastico si assume la responsabilità editoriale di garantire che il contenuto inserito dal personale autorizzato sia accurato e appropriato .

La comunicazione esterna online della scuola è coordinata e progettata per trasmettere all'esterno l'identità, i valori, le azioni, i progetti e l'idea di educazione che l'Istituto porta avanti.

La scuola è in grado di controllare l'accesso ai siti di social networking, nella pratica didattica si cerca di educare la componente studentesca al loro uso sicuro. Per esempio a ogni utente sarà consigliato di non fornire mai dati personali di alcun tipo che possano identificare con precisione le persone e la loro residenza o ubicazione.

La componente studentesca si deve astenere dall'utilizzo improprio di foto e/o materiale informativo pubblicato su social network e qualunque piattafoma utilizzata dalla scuola.

Alunne/alunni, genitori e personale docente e non docente saranno informati sull'uso sicuro degli spazi di social network e sulle conseguenze legali di ogni uso improprio.

Alunne e a Alunni al fine di consentire il riconoscimento, devono accedere alle piattaforme con il proprio nome e cognome (non con un nickname).

Per le comunicazioni formali ai docenti, l'Istituto utilizza, altri strumenti già consolidati (sito istituzionale, registro elettronico, mail).

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.

La componente studentesca è tenuta a rispettare le disposizioni qui riportate.

- I telefoni cellulari, i tablet e le relative fotocamere e registratori vocali non verranno utilizzati durante le lezioni scolastiche se non all'interno di attività didattiche espressamente programmate dal corpo docente e autorizzate dal Dirigente scolastico.
- L'alunno è tenuto a tenere spento il proprio dispositivo all'ingresso della scuola.
- Gli alunni con DSA,se previsto nel loro Piano personalizzato di apprendimento, potranno utilizzare gli strumenti compensativi quali tablet e computer portatili durante la lezione e dovranno spegnerli nel momento in cui essi non sono più necessari.
- Il mancato rispetto delle regole sull'utilizzo dei cellulari , tablet ecc. comporta che gli stessi vengano requisiti dal docente che ravvisa l'infrazione, depositati nella cassaforte della presidenza e consegnati al genitore/tutore che convocato, sarà contestualmente informato dell'eventuale sanzione disciplinare comminata al trasgressore.
- Nel caso in cui le alunne e o gli alunni debbano comunicare con la famiglia per questioni ,urgenti e inderogabi ,durante l'orario scolastico, possono usare gratuitamente la linea fissa della scuola rivolgendosi a un operatore; allo stesso modo le famiglie devono chiamare il centralino della scuola se hanno assoluta necessità di parlare con i propri figli. Si raccomanda di ridurre tali comunicazioni a casi di inderogabile necessità e urgenza.
- L'invio di materiali abusivi, offensivi o inappropriati, anche all'interno di cerchie o gruppi di discussione privati,è vietato e sanzionato secondo quanto stabilito dal Regolamento d'Istituto e fatte salve tutte le ulteriori conseguenze legali del caso.
- La ripresa non permessa di eventi, fatti e situazioni durante le attività didattiche è assolutamente vietata e sanzionata secondo quanto stabilito dal Regolamento d'Istituto e fatte salve tutte le uleriori conseguenze legali del caso .

Per il personale docente e ATA valgono le seguenti indicazioni.

- Il personale preferirà, quando ciò è possibile, l'impiego della strumentazione fornita dalla scuola rispetto a quella personale (portatili, pc fissi, …).
- Le infrastrutture e gli apparati della scuola non vanno utilizzati per scopi personali.
- Telefoni cellulari, tablet, fotocamere e altri strumenti di registrazione audio/video non devono essere impiegati durante le lezioni scolastiche se non all'interno di attività didattiche espressamente programmate e autorizzate.
- E' fatto divieto di utilizzare il proprio cellulare durante le ore di lezione per scopi non

didattici.

- La password di accesso alla rete wireless va custodita con cura e per nessuna ragione deve essere divulgata a chi non ha titolo per utilizzarla (studenti, genitori, operatori esterni).
- L'uso improprio della rete è contestato al titolare delle credenziali con cui è con cui è avvenuto l'accesso alla stessa.
- Qualora si utilizzino a scuola dispositivi di archiviazione esterna di proprietà personale (chiavette usb, dischi fissi portatili) è bene controllare preventivamente che essi siano esenti da virus per evitare di danneggiare le attrezzature comuni.

Durante l'attività didattica è opportuno, inoltre, che ogni docente:

- fornisca chiare indicazioni sul corretto utilizzo della rete (Internet, piattaforma studenti ecc.), condividendo con gli studenti la "netiquette" e indicandone le regole;
- vigili costantemente e diligentemente gli alunni durante le attività nei laboratori multimediali;
- segnali prontamente al tecnico informatico eventuali malfunzionamenti o danneggiamenti al tecnico informatico;
- eviti di salvare sulla memoria locale della postazione di classe file contenenti dati personali e/o sensibili;
- proponga agli alunni attività di ricerca di informazioni in rete fornendo opportunamente loro indirizzi dei siti e/o parole chiave per la ricerca.

Il nostro piano d'azioni

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

Scegliere almeno 1 di queste azioni

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte deglistudenti e delle studentesse.
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte dei docenti.
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte delpersonale Tecnico Amministrativo e dagli ATA.
- Organizzare uno o più eventi o attività volti a consultare i docenti dell'Istituto perredigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola.

- Organizzare incontri per la consultazione degli studenti/studentesse suindicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola.
- Organizzare incontri per la consultazione dei genitori su indicazioni/regolamentisull'uso dei dispositivi digitali personali a scuola.
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali.
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali.
- Organizzare uno o più eventi o attività volti a formare i genitori dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali.
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity).
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity).

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

Scegliere almeno 1 di queste azioni

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli studenti e delle studentesse.
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte dei docenti.
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte delpersonale Tecnico Amministrativo e dagli ATA.
- Organizzare uno o più eventi o attività volti a consultare i docenti dell'Istituto perredigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali.

- Organizzare incontri per la consultazione degli studenti/studentesse suindicazioni/regolamenti sull'uso dei dispositivi digitali personali.
- Organizzare incontri per la consultazione dei genitori su indicazioni/regolamentisull'uso dei dispositivi digitali personali.
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali.
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali.
- Organizzare uno o più eventi o attività volti a formare i genitori dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

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

4.1 - Sensibilizzazione e Prevenzione

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

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

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

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

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

Le principali aree di rischio possono essere riassunte come segue.

CONTENUTI

• L'esposizione a contenuti dannosi e non appropriati (es. contenuti razzisti ecc.).

• Siti web che promuovono stili di vita e comportamenti dannosi (es. siti che inneggiano al suicidio, che promuovono comportamenti alimentari scorretti, ecc.).

• Contenuti che spingono all'odio.

• Validazione dei contenuti: come controllare l'autenticità e l'esattezza dei contenuti online.

• Pornografia.

CONTATTI

• Grooming (adescamento online), sfruttamento sessuale.

• Cyberbullismo e bullismo in tutte le forme.

• Il furto di identità, comprese le password.

• Pedopornografia (con questo termine si intende qualsiasi foto o video di natura sessuale che ritrae persone minorenni).

CONDOTTE

• I comportamenti aggressivi (cyberbullismo e bullismo).

• Violazione della privacy, tra cui la divulgazione di informazioni personali o di dati (foto, video, voce) senza autorizzazione dei soggetti interessati.

REPUTAZIONE DIGITALE

• Salute e benessere: dipendenza da Internet e quantità di tempo speso online, gioco d'azzardo o gambling, videogiochi online in comunità mondiali, l'immagine del corpo.

• Sexting.

• Copyright (poca cura o considerazione per la proprietà intellettuale e i diritti d'autore).

Al fine di minimizzare i rischi e gli effetti di attacchi informatici legati all'utilizzo di postazioni di lavoro in rete, (sia essa Intranet o Internet), la scuola è dotata di

- comuni firewall, posizionati nel segmento di rete tra il router di accesso ad Internet e la rete interna in modo che si possa verificare tutto il traffico destinato o proveniente da reti esterne (Internet); esso è configurato per tenere traccia del traffico analizzato, tramite file di log, per successive indagini;
- antivirus che permettono di esaminare il traffico generato dalla navigazione internet e dalla posta elettronica alla ricerca di eventuali Virus Informatici; il server Antivirus (nome antivirus) è stato posizionato all'interno della LAN, ed opera, per il riconoscimento, sulla base di un archivio contenente le firme dei virus correntemente identificati;
- un sistema antivirus in dotazione a tutti i computer dei laboratori che permette di contrastare l'infezione dei PC da parte di virus informatici e trojan;
- un proxy server che regola l'accesso ai servizi internet; esso, funziona anche da memoria cache per la navigazione web, contribuisce all'aumento della velocità di navigazione, potendo restituire all'utente le pagine richieste già presenti nella propria memoria senza necessità di richiederle all'esterno;
- misure minime di sicurezza come da nota MIUR 0003015 del 20-12-2017;

- un controllo periodico delle postazioni informatiche dei laboratori con RESET di eventuali siti non didattici;
- un aggiornamento degli antivirus installati sulle macchine personali e controllo dei dispositivi di archiviazione esterna che vengano collegati al proprio pc.

Inoltre nei nostri tre plessi per prevenire azioni di bullismo o di ciberbullismo di e-policy in genere pensiamo di adottare

- una prevenzione rivolta a tutti tout-court;
- una prevenzione che sia rivolta a classi o gruppi di studenti che presentano un rischio potenziale;
- una prevenzione che interessi in modo attento coloro che sono coinvolti nel fenomeno.

Il tutto, riteniamo, non può avvenire senza una forte sinergia tra le famiglie e il personale scolastico tutto.

La rilevazione del clima di classe è la primissima azione preventiva. Le presunte vittime possono manifestare sintomi fisici o psicologici da leggere da subito come eventi di disagio e del problema.

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).

Gli alunni del nostro Istituto, vengono coinvolti in attività didattiche atte a sensibilizzarli circa i pericoli nascosti e palesi dei fenomeni in questione.

I docenti e il personale tutto vengono coinvolti con attività di formazione e preparazione per raggiungere quella sensibilità e capacità di comprendere il fenomeno.

La scuola partecipa a tutte quelle iniziative che vengono ritenute importanti e rilevanti per le problematiche in oggetto.

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.

Prevenire e/o contrastare: per riuscire a far emergere l' "hate speech" l'istituto "Beretta" reitera annualmente una serie di progetti che mirano all'Inclusione della diversità ed al rispetto con la creazione di un ambiente che favorisca la relazione tra pari,iniziative e attività sull'antisemitismo, così come percorsi di Educazione Civica integrata all'e-safety sulla salvaguardia dei diritti dell'uomo e del fanciullo.

4.4 - Dipendenza da Internet e gioco online

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

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

L'istituto Beretta promuove azioni con attività integrate con l'Agenda 2030, si pensi all'educazione digitale o alla cittadinanza digitale, affinchè internet e i suoi apparecchi connessi siano supporto ed integrazione alla quotidianità, e alla sociaità senza che il gioco e le attività ludiche del mondo della rete siano o creino dipendenze e patologie.

L'istituzione scolastica nel suo ruolo di trasmissione di conoscenza fornisce informazioni sulle varie tipologie di gioco on line e attua una prevenzione attraverso l'informazione e l'educazione dell'alunno all'uso consapevole di tutte le attività di gioco intese come momento di serenità e svago.

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.

Violenza psicosessuale, umiliazione, bullismo, cyberbullismo, molestie, stress emotivo che si riversa anche sul corpo insieme ad ansia diffusa, sfiducia nell'altro/i e depressione, questi rischi del sexting.

Le generazioni connesse di oggi non sono consapevoli di scambiare materiale che può avere conseguenze impattanti emotivamente per i protagonisti delle immagini, delle foto e dei video. Devono essere chiaro a tutti che scambiare foto o altro in modo sessualmente esplicito pone il ragazzo o la ragazza a conseguenze di difficile soluzione.

Il soggetto "sfruttatore" di questo comportamento diventa il "nemico" e non l'amico, la scuola deve anche fornire questa "consapevolezza" e conoscenza dei disturbi pscologici, sociali e relazionali che un cattivo utiizzo di social e siti di varia natura comporta.

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.

Sensibilizzare per contrastare tale fenomeno, capire inoltre il giovane e anticipare culturalmente il fenomeno.

Il miglior modo per prevenire casi di adescamento online è accompagnare ragazze e ragazzi in un percorso di educazione (anche digitale) all'affettività e alla sessualità. Ciò aiuterebbe a renderli più sicuri emotivamente.

È importante, inoltre, che ragazzi e ragazze sappiano a chi rivolgersi. Gli adulti coinvolti, genitori e docenti, devono essere un punto di riferimento per il minore che va compreso e ascoltato. Affinché ciò avvenga è necessario tenere sempre aperto un canale di comunicazione con loro sui temi dell'affettività, del digitale e della sessualità.

Fondamentale, inoltre, è portare avanti un percorso di educazione digitale che comprenda lo

sviluppo anche di capacità quali la protezione della propria privacy e la gestione dell'immagine e dell'identità online, la capacità di gestire adeguatamente le proprie relazioni online.

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.

La pedopornografia è un reato perseguibile d'ufficio e, come tale, se la realtà scolastica ne viene a conoscenza deve effettuare la denuncia all'autorità giudiziaria competente e garantire all'alunno, vittima di reato, il supporto psicologico.

In particolare il personale docente e in generale il personale scolastico, in presenza di reati perseguibili di ufficio, deve riferire al dirigente scolastico la notizia di reato di cui è venuto a conoscenza nell'esercizio delle sue funzioni. Spetterà poi al Drigente scolastico l'obbligo di denunciare la notizia di reato all'autorità giudiziaria competente.

Il nostro piano d'azioni

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

Scegliere almeno 1 di queste azioni

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

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

☐ Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti.

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

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

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

☐ Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/lle studenti/studentesse.

☐ Organizzare uno o più eventi e/o dibattiti in momenti 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.

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

Scegliere almeno 1 di queste azioni

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

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

☐ Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti.

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

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

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

☐ Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/lle studenti/studentesse.

☐ Organizzare uno o più eventi e/o dibattiti in momenti 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.

Le misure di prevenzione comprendono l'integrazione nel curricolo dei temi legati al corretto utilizzo delle TIC e di Internet: la progettazione di unità didattiche specifiche verranno pianificate a livello di dipartimenti disciplinari, garantendo interventi diversificati e contestualizzati in ogni classe.

La componente studentesca si può rivolgere per avere consigli e sostegno psicologico anche relativamente alle tematiche del cyberbullismo alle referenti dei tre plessi. Tuttavia, le/gli insegnanti in particolare sono chiamati a essere anche torre di avvistamento, spazio di avamposto privilegiato delle problematiche, dei rischi, dei pericoli che gli adolescenti possono vivere e affrontare ogni giorno.

Accorgersi tempestivamente di quanto accade e compiere azioni immediate di contrasto verso gli atti inopportuni - quando illegali - diviene fondamentale per poter evitare conseguenze a lungo termine che possano pregiudicare il benessere e una crescita armonica dei soggetti coinvolti.

Per i ragazzi nativi digitali le interconnessioni tra vita e tecnologia sono la normalità. Essi, pur essendo spesso tecnicamente competenti, tendono a non cogliere le implicazioni dei loro comportamenti e tale fenomeno è tanto maggiore quanto è più forte il coinvolgimento emotivo nell'utilizzo dei nuovi media. Ciò fa sì che alcuni rischi che fanno parte del mondo digitale possano non essere percepiti come tali ed è dunque compito degli adulti, famiglie ed insegnanti, affrontarli con l'obiettivo di prevenirli.

La gestione dei casi rilevati va differenziata a seconda della loro gravità; fermo restando che è opportuna la condivisione a livello di Consiglio di Classe di ogni episodio, anche minimo, alcuni avvenimenti possono essere affrontati e risolti con la discussione collettiva in classe. Altri casi ancora possono essere affrontati convocando genitori e alunno/a per riflettere insieme su quanto accaduto e come rimediare. Nei casi più gravi e in ogni ipotesi di reato occorre riferire tempestivamente al Dirigente Scolastico.

Come scuola vanno rilevati i:

- i comportamenti prepotenti e/o tutti quei comportamentii che hanno come obiettivo quello di danneggiare qualcuno in modo verbale, fisico o psicologico;
- gli elementi e materiali di vario genere postate in chat o social network;
- i contenuti che possano considerarsi in qualche modo lesivi: dell'onore, della reputazione e dell'immagine altrui;
- tutto ciò che rientra nella sfera sessuale: messaggi, immagini o video a sfondo sessuale.

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.

L’art.2 della L. n. 71/2017 prevede che il minore di quattordici anni, ovvero il genitore o altro soggetto esercente la responsabilità sul minore che abbia subito un atto di cyberbullismo, può inoltrare un'istanza per l'oscuramento, la rimozione o il blocco di qualsiasi dato personale del minore, diffuso nella rete:

 al titolare del trattamento

 al gestore del sito internet

 al gestore del social media.

Se entro ventiquattro ore dal ricevimento dell'istanza i soggetti responsabili non hanno comunicato di avere preso in carico la segnalazione, e entro quarantotto ore provveduto, l'interessato può rivolgere analoga richiesta, mediante segnalazione o reclamo, al Garante per la protezione dei dati

personali, il quale provvede entro quarantotto ore dal ricevimento della richiesta. http://www.garanteprivacy.it/cyberbullismo.

Inoltre,l'art. 7 della Legge 71/2017 prevede uno strumento d'intervento preventivo, già sperimentato in materia di atti persecutori (stalking), ovvero l'ammonimento del Questore.

Nello specifico, nel caso in cui non si ravvisino reati perseguibili d'ufficio o non sia stata formalizzata querela o presentata denuncia per le condotte di ingiuria (reato recentemente depenalizzato), diffamazione, minaccia o trattamento illecito dei dati personali commessi mediante la rete Internet nei confronti di altro minorenne, è possibile rivolgere al Questore, autorità provinciale di Pubblica Sicurezza, un'istanza di ammonimento nei confronti del minore ultraquattordicenne autore della condotta molesta. La richiesta potrà essere presentata presso qualsiasi ufficio di Polizia e dovrà contenere una dettagliata descrizione dei fatti, delle persone a qualunque titolo coinvolte ed eventuali allegati comprovanti quanto esposto.

E' bene sottolineare che l'ammonimento, in quanto provvedimento amministrativo, non richiede una prova certa e inconfutabile dei fatti, essendo sufficiente la sussistenza di un quadro indiziario che garantisca la verosimiglianza di quanto dichiarato. Qualora l'istanza sia considerata fondata, anche a seguito degli approfondimenti investigativi ritenuti più opportuni, il Questore convocherà il minore responsabile insieme ad almeno un genitore o ad altra persona esercente la potestà genitoriale, ammonendolo oralmente e invitandolo a tenere una condotta conforme alla legge con specifiche prescrizioni che, ovviamente, varieranno in base ai casi.

La legge non prevede un termine di durata massima dell'ammonimento ma specifica che i relativi effetti cesseranno al compimento della maggiore età.

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.

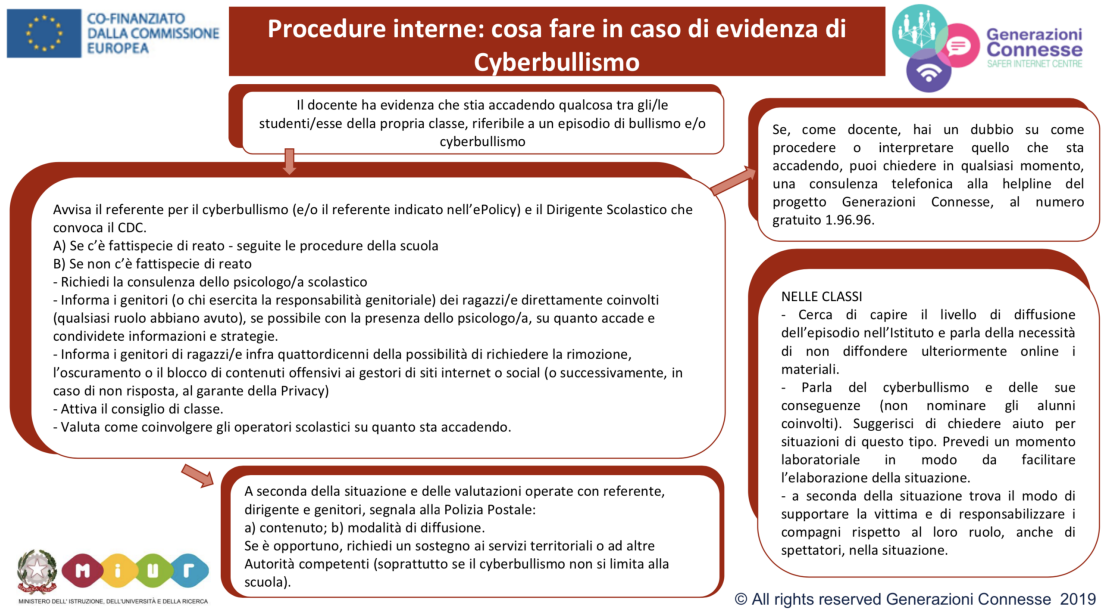
Importante è altresì ricordare il ruolo della Polizia Postale di Brescia, il Garante regionale per l'Infanzia e l'Adolescenza e il Tribunale dei Minori di Brescia, figure tutte con un importante ruolo per eventuali segnalazioni di particolare gravità.

Agli studenti e al personale scolastico docente e non docente è fatto divieto di utilizzare in modo improprio gli strumenti della scuola (Reti, Pc,….). Pertanto verrà segnalato all'autorità giudiziaria ogni accesso abusivo al sistema informatico ai sensi e nei limiti dell'art. 615 ter c.p. (utilizzo non autorizzato di strumenti , appropriazione password, blocco lim, ecc.).

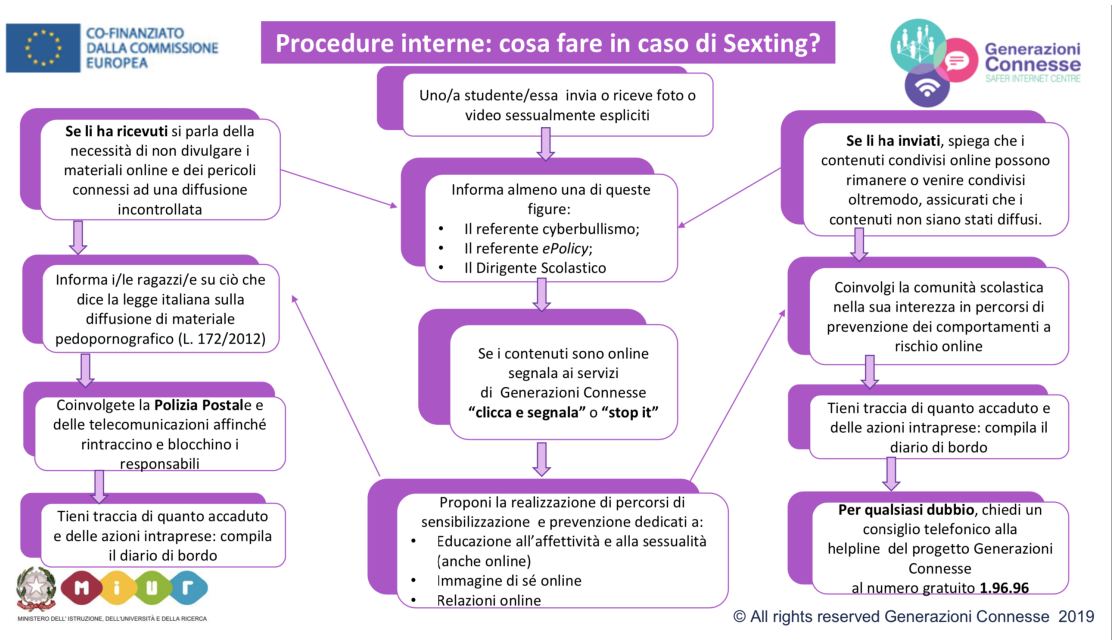
La nostra scuola ritiene importante il ruolo educativo e conoscitivo che le forze dell'ordine o enti specializzati e strutture possono svolgere all'interno del nostro istituto con incontri anche da remoto.

5.4. - Allegati con le procedure

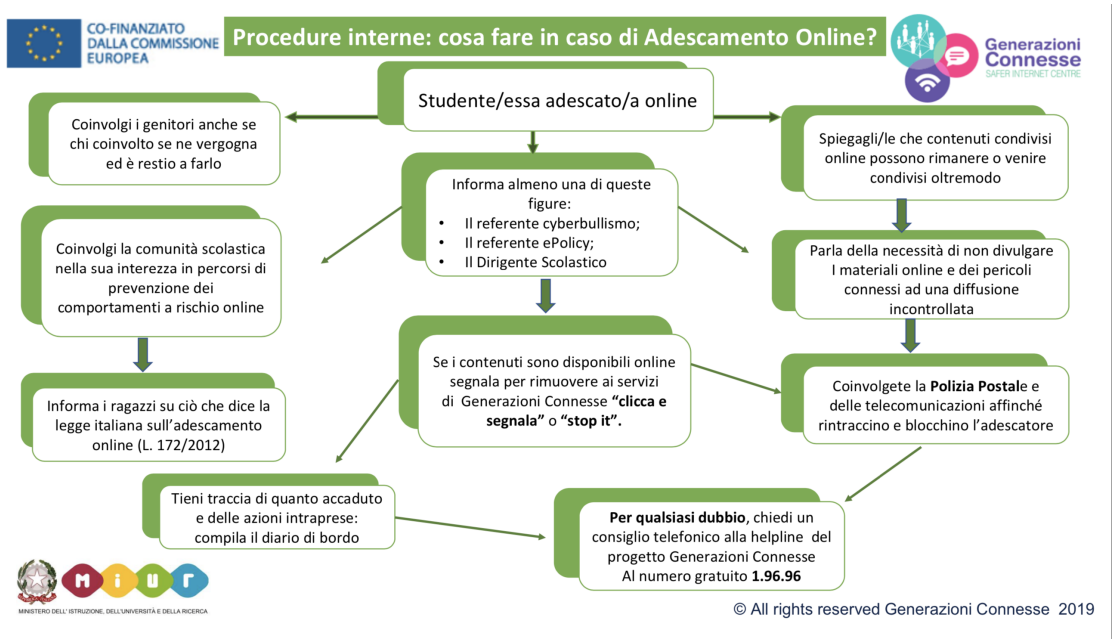
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



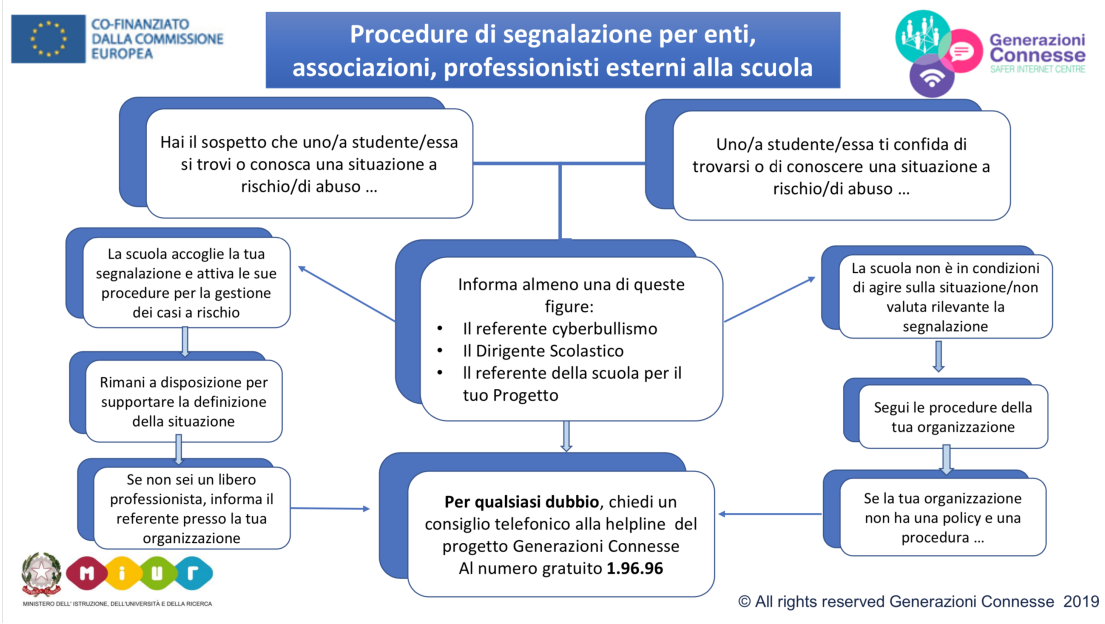
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



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



Altri allegati

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

Il nostro piano d'azioni

Non è prevista nessuna azione.