Documento di ePolicy

RMIC8A100A

IC MARINO CENTRO

VIA OLO GALBANI S.N.C. - 00047 - MARINO - ROMA (RM)

GIUSEPPE DI VICO

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.

La futura implementazione e le eventuali modifiche migliorative che saranno apportate al documento assumono ancora maggiore rilevanza in considerazione del fatto che l'Istituto Comprensivo Marino Centro, anticipando la Legge n. 71 del 29 maggio 2017 "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo", si è dotata sin dal 2015 di una struttura organizzativa di prevenzione e contrasto ai fenomeni del Bullismo e del Cyberbullismo, attraverso il progetto Scuola Attiva, tuttora operante. Sempre in quell'anno è stato vincitore di un Bando della Regione Lazio per l'attivazione di un percorso di formazione in rete, presentato in partenariato con l'Ambulatorio sulla Dipendenza da Internet del Policlinico Gemelli, che ha consentito la formazione intensiva sul fenomeno per i docenti. Dal 2016 l'IC Marino Centro è iscritto al Progetto del MIUR "Generazioni connesse" e nel 2018 riceve l'attestato di "Scuola Virtuosa". Dal 2015 ad oggi l'IC è attivo con servizi di supporto alle problematiche emotive e affettive dei ragazzi, dei genitori e dei docenti con percorsi specifici di formazione e prevenzione.

Il documento potrà dunque, se necessario, essere modificato e aggiornato annualmente in funzione di eventuali nuove esigenze e, di conseguenza, di nuove azioni da porre in essere anche nell'ottica di una sua piena integrazione con obiettivi e contenuti degli altri documenti di Istituto, primo tra tutti il PTOF.

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	• Responsabilità generale per i dati e la sicurezza degli stessi • Accertarsi che la scuola utilizzi un Internet Service filtrato approvato, conforme ai requisiti di legge vigenti; • La responsabilità di assicurare che il personale riceva una formazione adeguata per svolgere i ruoli di sicurezza online e per la formazione di altri colleghi; • Essere a conoscenza delle procedure da seguire in caso di infrazione della E-Safety Policy; • Controllare e disporre aggiornamenti sulla E-Safety Policy; • Ricevere relazioni di monitoraggio periodiche della sicurezza online da parte del responsabile; • Gestire le segnalazioni ai Servizi Sociali; • Monitorare l'utilizzo corretto di Workspace. • Essere formato adeguatamente sulla sicurezza e sulla prevenzione di problematiche offline e online, in linea con il quadro normativo di riferimento e le indicazioni del MIUR; • Essere promotore della cultura della sicurezza online e, ove possibile, dare il proprio contributo all'organizzazione, insieme al docente referente sulle tematiche del bullismo/cyberbullismo, di corsi di formazione specifici per tutte le figure scolastiche sull' utilizzo positivo e responsabile delle TIC. • E' responsabile di gestire ed intervenire nei casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali.

REFERENTE CONTRO IL BULLISMO E IL CYBERBULLISMO

• Coordinare le iniziative di prevenzione e di contrasto del cyberbullismo, anche avvalendosi della collaborazione delle Forze di polizia nonché delle associazioni e dei centri di aggregazione giovanile presenti sul Territorio (L. 71/2017, art. 4, c. 3);
• Raccogliere e diffondere le buone pratiche educative, organizzative e azioni di monitoraggio;
• Supporto al dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d'istituto), atti e documenti (PTOF, PdM, Rav). (Linee di orientamento);
• Promuovere la consapevolezza e l'impegno per la salvaguardia online in tutta la comunità scolastica;
• Garantire che tutto il personale sia a conoscenza delle procedure che devono essere seguite in caso di incidente per la sicurezza online;
• Garantire che sia tenuto un registro di incidente di sicurezza online;
• Garantire che sia dedicata e costantemente aggiornata una bacheca informativa, in ogni Plesso della Scuola, dedicata agli alunni e ai genitori;
• Garantire la massima diffusione ai docenti, genitori e alunni, dei contenuti di prevenzione e contrasto ai fenomeni;
• Controllare che sia posto in ogni Plesso una cassetta per le segnalazioni e pubblicizzata la mail dedicata;
• Facilitare la formazione e la consulenza per tutto il personale;
• Coordinare interventi con le autorità locali e le agenzie competenti;
• Facilitare la creazione di Reti significative e funzionali con il territorio;
• Raccordarsi con il Dirigente Scolastico e il suo staff;
• Accogliere e supportare i genitori e gli alunni in difficoltà;
• Patrocinare gli interventi di formazione e prevenzione con le ASL e Enti Territoriali;
• Monitorare l'utilizzo corretto di Workspace;

TEAM ANTIBULLISMO E PER LE EMERGENZE

• Monitorare la sicurezza online nel Proprio Plesso;
• Raccogliere le schede di prima segnalazione dei docenti
• Compilare la scheda di valutazione approfondita
• Esaminare casi segnalati e coordinare gli interventi;
• Promuovere la consapevolezza e l'impegno per la salvaguardia online tra gli alunni, i genitori e il personale scolastico;
• Garantire che tutto il personale del Plesso sia a conoscenza delle procedure che devono essere seguite in caso di incidente per la sicurezza online;
• Garantire che sia tenuto un registro di Plesso per eventuali incidenti riguardanti la sicurezza online;
• Facilitare la formazione e la consulenza per il personale del Plesso;
• Coordinare gli interventi con lo staff, il Dirigente e il Referente d'Istituto per il Bullismo e Cyberbullismo;
• Monitorare l'applicazione delle norme sulla condivisione dei dati personali;
• Monitorare e segnalare l'accesso a materiali illegali o inadeguati;
• Controllare, gestire e segnalare probabili azioni di cyberbullismo;
• Applicare ognuno nella propria sede di lavoro le disposizioni di legge previste e le azioni di prevenzione e contrasto decise dall'Istituto;
• Garantire che sia dedicata e costantemente aggiornata una bacheca informativa, nel proprio Plesso, dedicata agli alunni e ai genitori;
• Garantire la massima diffusione ai docenti, genitori e alunni, dei contenuti di prevenzione e contrasto ai fenomeni;
• Esporre, in maniera visibile, una cassetta per le segnalazioni e pubblicizzata la mail dedicata;
• Accogliere e consigliare i genitori e gli alunni in difficoltà;
• Monitorare l'utilizzo corretto di Workspace nel proprio Plesso;
• Supportare i docenti di classe, i genitori e il personale scolastico.

L'ANIMATORE DIGITALE E IL TEAM DIGITALE	• Pubblicare la E-Policy sul sito della scuola; • Pubblicare le iniziative di Scuola Attiva sul sito della scuola; • Assistenza ai docenti per il controllo alla corretta navigazione; • Diffusione delle netiquette sull'uso responsabile di internet; • Diffusione della conoscenza di materiali per uso didattico in CC, Creative Commons e software open source; • Verifica dell'aggiornamento costante dell'antivirus e eliminazione applicazioni non autorizzate; • Promuovere la formazione per i docenti e i genitori sulle tematiche in oggetto; • Amministrare, gestire e monitorare l'utilizzo corretto di Workspace. • Coordinare con la Funzione Area 6 gli interventi dell'assistente tecnico in merito alla sicurezza digitale dei dispositivil • Supportare il personale scolastico da un punto di vista non solo tecnico-informatico e in riferimento ai rischi online, alla protezione e gestione dei dati personali; • Essere uno dei promotori di percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale" (con riferimento allo sviluppo delle competenze digitali previste anche nell'ambito dell'educazione civica); • Monitorare e rilevare eventuali episodi o problematiche connesse all'uso delle TIC a scuola; • Controllare che gli utenti autorizzati accedano alla Rete della scuola con apposita password, per scopi istituzionali e consentiti (istruzione e formazione).

GLI INSEGNANTI	• Integrare parti del curriculum della propria disciplina con approfondimenti ad hoc, promuovendo, laddove possibile, anche l'uso delle tecnologie digitali nella didattica. • Inserire tematiche legate alla sicurezza online in tutti gli aspetti del programma di studi e di altre attività scolastiche; • Coltivare quotidianamente all'interno della didattica le buone pratiche al benessere digitale; • Supervisionare e guidare gli alunni con cura quando sono impegnati in attività di apprendimento che coinvolgono la tecnologia online; • Garantire che gli alunni siano pienamente consapevoli delle capacità di ricerca e dei problemi legali relativi ai contenuti elettronici come ad esempio le leggi sul copyright; • Segnalare **obbligatoriamente** al membro del Team Antibullismo del proprio plesso, attraverso la scheda di prima segnalazione, eventuali casi di bullismo, cyberbullismo o violazioni in rete di cui si è venuto a conoscenza o se ne sospetta l'esistenza; • Formarsi sulle tematiche del cyberbullismo e della dipendenza da internet; • Diventare un punto di riferimento per i propri alunni in quanto a prevenzione, supporto e informazione.; • Utilizzo corretto di Workspace e delle TIC e monitoraggio dell'uso da parte dei propri alunni. • Accompagnare e supportare gli studenti e le studentesse nelle attività di apprendimento e nei laboratori che prevedono l'uso della LIM o di altri dispositivi tecnologici che si connettono alla Rete;
IL PERSONALE SCOLASTICO (ATA)	• Comprendere e contribuire a promuovere politiche di e-sicurezza; • Essere consapevoli dei problemi di sicurezza online connessi con l'uso di telefoni cellulari, fotocamere e dispositivi portatili; • Monitorare l'uso di dispositivi tecnologici e attuare politiche scolastiche per quanto riguarda questi dispositivi; • Segnalare qualsiasi abuso sospetto o problema al Team Antibullismo; • Usare comportamenti sicuri, responsabili e professionali nell'uso delle tecnologie; • Garantire che le comunicazioni digitali con gli studenti siano solo a livello professionale e solo attraverso sistemi scolastici, non attraverso chat o mail personali; • Utilizzo corretto di Workspace.

LE STUDENTESSE E GLI STUDENTI

• Leggere, comprendere ed accettare la E-Safety Policy;
• Conoscere e rispettare le leggi sulla privacy e sul copyright;
• Capire l'importanza di segnalare abusi, minacce, atti di cyberbullismo o accesso a materiali inappropriati;
• Sapere quali azioni intraprendere se loro, o qualcuno che conoscono, si sente preoccupato o vulnerabile riguardo le nuove tecnologie;
• Conoscere e rispettare la politica della scuola relativa all'uso dei telefoni cellulari, tablet, fotocamere digitali e dispositivi portatili;
• Conoscere e capire la politica della scuola sull'uso di immagini e sul cyberbullismo;
• Capire l'importanza di adottare buone pratiche di sicurezza online quando si usano le tecnologie digitali fuori dalla scuola;
• Assumersi la responsabilità di conoscere i benefici e i rischi di utilizzo di internet e di altre tecnologie in modo sicuro,sia a scuola che a casa;
• Utilizzo corretto di Workspace.
• Utilizzare al meglio le tecnologie digitali in coerenza con quanto richiesto dai docenti; con il supporto della scuola dovrebbero **imparare a tutelarsi online.**
• Tutelare i/le propri/e compagni/e e rispettarli/le;
• Partecipare attivamente a progetti ed attività che riguardano l'uso positivo delle TIC e della Rete e farsi promotori di quanto appreso anche attraverso possibili percorsi di peer education;

I GENITORI

• Essere partecipi e attivi nelle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete, nonché sull'uso responsabile dei device personali;
• Relazionarsi in modo costruttivo con i docenti sulle linee educative che riguardano le TIC e la Rete e comunicare con loro circa i problemi rilevati quando i/le propri/e figli/e non usano responsabilmente le tecnologie digitali o Internet.
• **È estremamente importante che accettino e condividano quanto scritto nell'ePolicy dell'Istituto.**
• Genitori e tutori si impegnano a garantire che i loro figli comprendano la necessità di utilizzare i dispositivi digitali e la rete in modo appropriato;
• Genitori e tutori si impegnano a partecipare attivamente agli eventi organizzati dalla scuola per la promozione delle buone pratiche di e-safety e la prevenzione o il contrasto del cyberbullismo;
• Genitori e tutori si impegnano nel promuovere le buone pratiche di e-safety e a seguire le linee guida sull'uso appropriato di:
- Immagini digitali e video registrati in occasione di eventi scolastici, anche al di fuori delle aule;
- Accesso alle sezioni del sito dedicate ai genitori, con particolare riguardo al registro elettronico;
- Dispositivi personali dei loro figli nella scuola;
- Monitorare l'utilizzo corretto di Workspace del proprio figlio.

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

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

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

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

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

Il documento di E-policy viene condiviso con tutta la comunità educante, ponendo al centro gli studenti e le studentesse e sottolineando compiti, funzioni e attività reciproche. È molto importante che ciascun attore scolastico (dai docenti agli/lle studenti/esse) si faccia a sua volta promotore del documento.

L’E-policy viene condivisa e comunicata al personale, agli studenti e alle studentesse, alla comunità scolastica attraverso:

- la pubblicazione del documento sul sito istituzionale della scuola;
- il Patto di Corresponsabilità, che deve essere sottoscritto dalle famiglie e rilasciato alle stesse all’inizio dell’anno scolastico;

Il documento è approvato dal Collegio dei Docenti e dal Consiglio di Istituto e viene esposto in versione semplificata negli spazi che dispongono di pc collegati alla Rete o comunque esposto in vari punti spaziali dell'Istituto.

Gli studenti e le studentesse vengono informati sul fatto che sono monitorati e supportati nella navigazione on line, negli spazi della scuola e sulle regole di condotta da tenere in Rete.

Il presente documento sarà pubblicato sul sito web della scuola, nella sezione dedicata alle azioni di contrasto al Bullismo/Cyberbullismo, ed integrato, come allegato, nel PTOF (Piano Triennale per l'Offerta Formativa). Ciò garantirà una completa condivisione da parte dell'intera comunità scolastica e potrà rendere il documento una base di partenza per azioni e iniziative, quali una discussione aperta sui contenuti e sulle pratiche indicate, sulle modalità per inserire le tematiche di interesse della Policy nel curricolo, nonché un confronto in merito alla necessità di apportarvi modifiche e miglioramenti.

L'E-Policy d'Istituto si applica a tutti i membri della scuola, compreso il personale, gli studenti, i genitori, gli utenti della comunità che ne hanno accesso.

La Policy sarà comunicata al personale, agli alunni, alla comunità nei seguenti modi:

- Pubblicazione della EPolicy sul sito della scuola;
- Tramite il Patto di Corresponsabilità, che sarà sottoscritto dalle famiglie all'inizio dell'anno scolastico o nel momento di iscrizione all'I.C.;
- Diffusione dell'E-Safety Policy in sede di: Consiglio d'Istituto, GLI, Collegio dei docenti, Consigli di Classe, Consigli di Intersezione, Consigli di Interclasse.

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.

Il Dirigente Scolastico regola il comportamento degli studenti e autorizza i membri del personale a imporre sanzioni disciplinari per il comportamento inadeguato. Questo è pertinente a episodi di cyberbullismo, o altri tipi di incidenti che possono danneggiare la sicurezza online. I provvedimenti disciplinari nei confronti dell'alunno che ha commesso un'infrazione alla policy sono esplicitati nel Regolamento di Disciplina.

La scuola, attraverso i singoli Consigli di Classe e Team, si occuperà di tali incidenti all'interno di questa Policy, delle politiche di comportamento e antibullismo associati, e nel quadro normativo del Regolamento di Disciplina dell'Istituto e dello "Statuto degli Studenti e delle Studentesse", DPR 24 giugno 1998, n. 249, e avrà il compito di informare i genitori di episodi di comportamento inappropriato di sicurezza online, che si svolgono all'interno della scuola.

Per episodi segnalati, ma accaduti in spazi e tempi extrascolastici, la scuola informerà e coinvolgerà in ogni caso i genitori.

Qualora tali infrazioni dovessero configurarsi come reato, se ne sarà data tempestiva segnalazione al Dirigente Scolastico per gli adempimenti del caso. Infatti 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).

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.

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.

La E-Policy sarà riesaminata ogni due anni o quando si verificano cambiamenti significativi per quanto riguarda le tecnologie in uso all'interno della scuola e tutte le modifiche della Policy saranno discusse in dettaglio con tutti i membri del personale docente.

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.

Nell'ambito del PNSD questa scuola si propone un programma di progressiva educazione alla sicurezza online come parte del curriculum scolastico. Si impegna a sviluppare una serie di competenze e comportamenti adeguati all'età degli alunni e ad esperienza, tra cui:

• Programmare attività e far partecipare gli alunni a laboratori specifici sul digitale e la sicurezza in rete;

• Sviluppare una serie di strategie per valutare e verificare le informazioni prima di accettare l'esattezza;

• Essere a conoscenza delle fonti delle notizie in rete e che l'autore di un post o un sito web/pagina può avere un particolare pregiudizio;

• Sapere come restringere o affinare una ricerca;

• Riconoscere un comportamento accettabile quando si utilizza un ambiente online, vale a dire, essere educato, non utilizzare comportamenti inappropriati, mantenere le informazioni personali private;

• Conoscere e seguire la netiquette;

• Capire come le fotografie possono essere manipolate e individuare contenuti web in grado di attrarre il tipo sbagliato di attenzione;

• Comprendere l'esistenza e saper riconoscere i profili fake e le false identità degli interlocutori in chat e social network;

• Capire il motivo per cui non dovrebbero inviare o condividere resoconti dettagliati delle loro vite personali e informazioni di contatto;

• Capire il motivo per cui non devono pubblicare foto o video di altri senza permesso; • Comprendere la motivazione del divieto di utilizzo dei cellulari a scuola;

• Comprendere l'importanza di non scaricare file, software coperti da copyright o di dubbia natura;

• Conoscere e contrastare i fenomeni di bullismo e cyberbullismo in tutte le sue forme;

• Sapere come chiedere aiuto e segnalare atti di bullismo e cyberbullismo;

• Utilizzare con attenzione Internet per garantire che si adatti alla loro età e supporti gli obiettivi di apprendimento per le aree curricolari specifiche;

• Conoscere e saper utilizzare positivamente le potenzialità delle nuove tecnologie e del mondo digitale;

• Conoscere le risorse digitali nel complesso, non esclusivamente legate al lato applicativo.

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.

Nell'ambito del PNSD questa scuola ha previsto:

• Nomina di un Animatore Digitale e di un Team Digitale, con rappresentanti di tutti i plessi dell'Istituto, che accompagnerà il Dirigente Scolastico e il DSGA nell'attuazione degli obiettivi e delle innovazioni previste dal PNSD

• Formazione dei docenti all'utilizzo delle TIC, in particolare nell'utilizzo di Workspace.

• Autoformazione dei docenti con tutorial pubblicati sul sito internet della scuola.

• Si assicura che il personale sa come inviare o ricevere dati sensibili o personali e comprendere l'obbligo di crittografare i dati dove la sensibilità richiede protezione degli stessi

• Offre una formazione a disposizione del personale in materia di sicurezza online attraverso corsi di aggiornamento

• Fornisce informazioni a tutto il nuovo personale circa le indicazioni presenti sulla E-Safety Policy d'Istituto.

- Supporto e assistenza del team digitale ai docenti

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.

Da implementare con le indicazioni contenute nella lezione.

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.

Questa scuola esegue un programma continuativo di consulenza, orientamento e formazione per i genitori, tra cui:

• Presentare ai genitori il Regolamento della Policy, al fine di garantire che i principi di comportamento sicuro online siano chiari ;

• Bacheche informative e dedicate in ogni Plesso ;

• Mail a disposizione per i genitori e gli alunni per informazioni, segnalazioni e supporto all'indirizzo teamantibullismo@icmarinocentro.edu.it ;

• Offrire incontro di consulenza con lo staff del team antibullismo;

• Sezione dedicata sul sito internet della scuola;

• Fornire informazioni sui siti nazionali di sostegno per i genitori, quali il sito

www.generazioniconnesse.it ;

• Sportello psicologico gratuito;

• Corsi di formazione per i genitori sulle tematiche della corretta navigazione.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2023/2024)

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 allega l'informativa sul trattamento dei dati personali degli studenti e delle famiglie.

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.

La scuola garantisce a tutti gli utenti il diritto a internet attraverso un'infrastruttura di rete adeguata al numero di studenti e in grado di supportare il traffico dati generato da un numero elevato di utenti. La connessione è in fibra ottica ed è cablata sull'intero istituto.

L'infrastruttura di rete nell'istituto è così organizzata:

Rete LAN

L'istituto, nella sede centrale, dispone di un dominio su rete locale (rete segreteria) cui accedono i computer dell'amministrazione, tali postazioni sono su una rete locale isolata dal resto della rete d'Istituto (rete didattica).

Una linea LAN è dedicata esclusivamente al computer del Dirigente Scolastico. Il collegamento di computer portatili o palmari personali alla rete d'Istituto deve essere autorizzato dal Dirigente Scolastico. Tutte le sedi sono provviste di Rete LAN. La rete interna è protetta da Firewall per quanto riguarda le connessioni con l'esterno. Le postazioni sono protette con sistemi antivirus e antimalware regolarmente aggiornati. La memorizzazione dei documenti e delle impostazioni personali è garantita attraverso il meccanismo di profili mobili di Windows, che archivia centralmente sul server di dominio i dati, e li rende disponibili in tutte le postazioni legate alla didattica (laboratori, sale insegnanti, classi). Su questi dispositivi non è garantito alcun servizio di backup, pertanto si consiglia di fare copia su un supporto personale.

Per quanto concerne la rete amministrativa, lo storage è garantito da backup automatico su Cloud.

Rete senza fili (Wireless-WIFI)

L'Istituto, in tutti i suoi plessi, dispone di una rete con tecnologia senza fili. L'accesso alla rete wireless è regolamentato dalla chiave di accesso. L'ottenimento della chiave d'accesso è riservato solo agli autorizzati. Le regole di comportamento sono analoghe a quelle per la connessione alle reti cablate dell'Istituto.

Utilizzo della rete da parte di studenti e personale scolastico:

Come da regolamento sull'uso delle TIC gli studenti si impegnano a:

- utilizzare la rete nel modo corretto
- rispettare le consegne dei docenti
- non scaricare materiali e software senza autorizzazione
- non utilizzare unità rimovibili personali senza autorizzazione
- tenere spento il dispositivo al di fuori delle attività didattiche che ne prevedano l'utilizzo specifico
- durante le attività che prevedono l'uso del tablet, utilizzarlo esclusivamente per svolgere le attività didattiche previste

I docenti si impegnano a:

- utilizzare la rete nel modo corretto
- non utilizzare device personali se non per fini didattici e istituzionali (Compilazione del Registro Elettronico, ricerche didattiche, consultazione siti istituzionali, ecc.).
- formare gli studenti all'uso della rete
- dare consegne chiare e definire gli obiettivi delle attività
- monitorare l'uso che gli studenti fanno delle tecnologie a scuola.

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.

La scuola adotta per tutto il personale e gli studenti Google Workspace, una piattaforma integrata a marchio Google che consente di comunicare e di gestire contenuti digitali con grande semplicità e flessibilità. Le apps di Google garantiscono sicurezza e privacy, connessione e interoperabilità, comunicazione facilitata tra docenti e studenti.

Tutti gli studenti hanno accesso ad una serie di servizi, tra i quali:

• G-mail personale con spazio di archiviazione;

• Google Drive, che permette di archiviare online tutti i tipi di file, senza limiti di spazio;

• Google Classroom, per avere una classe virtuale nella quale lavorare attivamente e ricevere materiale aggiuntivo da parte degli insegnanti.

Gli studenti ed i genitori devono tuttavia sapere, nel momento in cui ricevono le credenziali di accesso e dopo aver accettato la presente informativa, che i servizi offerti sono ESCLUSIVAMENTE per utilizzo scolastico e didattico. L'utilizzo di Google Workspace è indispensabile per realizzare l'azione didattica programmata nel PTOF di Istituto. Le famiglie devono concedere l'autorizzazione alla creazione dell'account e all'utilizzo della piattaforma Google Workspace da parte dei figli compilando apposita liberatoria disponibile sul sito d'Istituto. Nel momento in cui gli account degli studenti vengono creati e attivati, i genitori sono responsabili della vigilanza sull'utilizzo degli account scolastici a casa e sui dispositivi personali degli studenti, in particolare sull'utilizzo degli account per finalità esclusivamente didattiche e in accordo con i docenti. È vietato, ad esempio, utilizzare il proprio account scolastico per registrarsi su piattaforme di gioco o sui social network a uso personale.

Questa scuola ha predisposto per tutto il personale e per tutti gli alunni una mail istituzionale @icmarinocentro.edu.it, fornito da Google Workspace, che diventa l'unico canale autorizzato di invio comunicazioni tramite mail, eccezion fatta per la mail ufficiale rmic8a100a@istruzione.i. Questa scuola non pubblica indirizzi di posta elettronica personali degli alunni o del personale sul sito della scuola, eccezion fatta per mail istituzionali di area.

Ogni mail segnalata come non appropriata sarà vagliata dal Dirigente Scolastico e, ove si riscontrassero presunte infrazioni di legge, queste mail saranno segnalate alle autorità competenti. Mail di spam, di phishing, virus e malware allegati possono risultare particolarmente pericolose. Perciò si utilizzeranno una serie di tecnologie per proteggere utenti e sistemi nella scuola, tra cui Antivirus e antimalware.

Quando possibile, i pc della scuola sono programmati per effettuare gli aggiornamenti periodici sia del software che del Sistema operativo.

I docenti sono tenuti a tenere aggiornati e ordinati i pc di classe, anche cancellando con frequenza dati sensibili e documenti/software superflui. Essi sono inoltre invitati a non salvare su pc collocati in aree comuni (es. aula docenti) file personali o contenenti dati personali degli alunni. L'unico sistema di archiviazione consentito sui pc della scuola è il Drive personale del docente.

La scuola garantisce formazione adeguata allo staff, incluso il corpo docenti sulla gestione dei dispositivi e sulle regole basilari sulla sicurezza.

Policy sulle password: le password devono essere forti:

- Le password non devono essere facilmente identificabili (nomi dei figli, compleanni, etc.).
- Le password non devono essere memorizzate nei dispositivi scolastici.
- Le password non devono essere condivise con nessuno.

Si allega il regolamento sull'uso delle tecnologie a scuola (policy di uso accettabile).

Strumenti di comunicazione online che possono essere utilizzati a scuola:

Comunicazione interna: strumenti utilizzati dalla scuola, sia per raggiungere target esterni, al fine di valorizzare e promuovere le attività portate avanti dall'Istituto, sia per far circolare all'interno della scuola informazioni di servizio o contenuti importanti fra i diversi attori scolastici:

Sito web della scuola:

L'istituto dispone di un sito web e di un proprio dominio https://www.icmarinocentro.edu.it L'istituto gestisce un proprio sito web nello spazio di proprietà. La gestione del sito della scuola e la rispondenza alle normative per quanto concerne i contenuti (accuratezza, appropriatezza, aggiornamento e accessibilità) e le tecniche di realizzazione e progettazione è a cura del webmaster. La scuola detiene i diritti d'autore dei documenti che si trovano sul proprio sito o di quei documenti per i quali è stato chiesto ed ottenuto il permesso dell'autore proprietario. Le informazioni pubblicate sul sito della scuola relativo alle persone da contattare rispetteranno le norme vigenti sulla privacy.

La scuola, in qualità di ente pubblico, pubblicherà sul proprio sito web i contenuti che saranno valutati come pertinenti alle finalità educative istituzionali, ponendo attenzione alla tutela della privacy degli studenti e del personale, secondo le disposizioni normative.

Comunicazione esterna: hanno lo scopo di facilitare e rendere più partecipata la didattica e la comunicazione a scuola: registro elettronico, email istituzionale, app di

Google Workspace.

In riferimento all'uso degli strumenti di comunicazione online per la circolazione di informazioni e comunicazione interne, come avviene generalmente fra i docenti mediante ad esempio l'uso di gruppi Whatsapp, è importante ricordare quello che si può definire "diritto alla disconnessione" (art.22 - Livelli, soggetti, materie di relazioni sindacali per la Sezione Scuola del CCNL 2016/2018).

Per le chat informali fra colleghi non esiste una vera e propria regolamentazione, e per tale ragione si stabiliscono le seguenti regole condivise sull'uso:

- Mettere in chiaro fin dall'inizio, comprendere e rispettare sempre le finalità del gruppo, scrivendo e pubblicando solo contenuti pertinenti a tali finalità;
- Usare sempre un linguaggio adeguato e il più possibile chiaro e preciso (come già sottolineato la comunicazione online si presta spesso a non pochi fraintendimenti);
- Evitare di affrontare in chat argomenti troppo complessi e controversi (la comunicazione online in una chat di gruppo non è adatta per la gestione di problematiche di questo tipo, che certamente è più opportuno affrontare in presenza o in un Consiglio di classe);
- Evitare discussioni di questioni che coinvolgono due o pochi interlocutori, onde evitare di annoiare e disturbare gli altri componenti del gruppo;
- Indirizzare solo domande precise e chiare, a cui si possano dare risposte altrettanto brevi e precise;
- Evitare messaggi troppo spezzettati, cercando il più possibile di essere brevi ed esaustivi allo stesso tempo.

Il registro elettronico permette di gestire la comunicazione con le famiglie, le quali attraverso di esso possono visualizzare molte informazioni utili, interagendo con la scuola, su:

- andamento scolastico (assenze, argomenti lezioni e compiti, note disciplinari);
- risultati scolastici (voti, documenti di valutazione);
- udienze (prenotazioni colloqui individuali);

- circolari e comunicazione varie (comunicazioni di classe, comunicazioni personali).

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.

Strumentazione personale

a. Per gli studenti:

Come da Regolamento d'Istituto agli studenti è vietato l'utilizzo del cellulare all'interno della scuola. Per quanto concerne l'utilizzo del tablet o del pc, questi possono essere utilizzati solo in presenza del docente e per ragioni prettamente didattiche.

A proposito dell'utilizzo di telefoni cellulari e di altri dispositivi elettronici durante l'attività didattica quando autorizzato dal docente, il discente ha il dovere di

- assolvere assiduamente agli impegni di studio anche durante gli orari di lezione;
- di tenere comportamenti rispettosi degli altri;
- di osservare le disposizioni organizzative dettate dai regolamenti di istituto

La famiglia deve impegnarsi a rispondere direttamente dell'operato dei propri figli nel

caso in cui, ad esempio, gli stessi arrechino danni ad altre persone o alle strutture scolastiche o, più in generale, violino i doveri sanciti dal regolamento di istituto.

Dirigente, docenti e personale ATA hanno il dovere di vigilare sui comportamenti degli studenti e delle studentesse il quale sussiste in tutti gli spazi scolastici e di segnalare eventuali infrazioni suscettibili di sanzioni disciplinari.

In virtù della normativa vigente posta a tutela della privacy, è fatto divieto di utilizzo di telefoni cellulari o di altri dispositivi elettronici nelle comunità scolastiche allo scopo di acquisire, divulgare e/o pubblicare immagini, filmati o registrazioni vocali senza il consenso esplicitamente espresso in forma scritta dagli interessati o i loro tutori (nel caso di minori). In altre parole, è punibile sia a livello civile che penale (oltre che le sanzioni previste dagli artt. 3 e 4, d.P.R. 24 giugno 1998, n. 249 - "Regolamento recante lo statuto delle studentesse e degli studenti della scuola secondaria"), chi abusa dei dati personali altrui raccolti (immagini, filmati, registrazioni vocali…), violandone la privacy.

b. Per i docenti e il personale scolastico:

I docenti e il personale della scuola possono utilizzare smartphone e tablet esclusivamente a fini didattici e istituzionali (Compilazione del Registro Elettronico, ricerche didattiche, consultazione siti istituzionali, ecc.).

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2023/2024).

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 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.*

Questo implica:

- una formazione del personale e delle famiglie sulla sicurezza e sulla prevenzione di problematiche offline e online, in linea con il quadro normativo di riferimento e le indicazioni del MIUR e lo sviluppo di servizi rivolti ai/alle ragazzi/e dal contenuto

innovativo e di più alta qualità, che garantiscano loro di muoversi in sicurezza e con competenza negli ambienti digitali.

- l'individuazione di un referente, e di un *team*, che coordini le iniziative di prevenzione e di contrasto dei pericoli *on-line* partendo da una consapevolezza, conoscenza e preparazione per un uso consapevole delle tecnologie digitali.

La **sensibilizzazione** può costituire il primo passo verso un cambiamento positivo, ma per far sì che l'intervento sia efficace, è importante che sia chiara l'azione verso cui i soggetti devono impegnarsi. Tre sono gli aspetti che bisogna tenere in considerazione:

- spingere le persone a desiderare un cambiamento;
- porre in evidenza la possibilità di generare un cambiamento;
- individuare le azioni che consentono di produrre il cambiamento.

Per quanto riguarda la **prevenzione** ne esistono 3 livelli:

- Prevenzione Universale. Un programma di questo tipo parte dal presupposto che tutti gli studenti siano potenzialmente a rischio. Si tratta quindi di interventi diretti al grande pubblico o a un intero gruppo di una popolazione che non è stato identificato sulla base del rischio individuale. Efficacia: trattandosi di programmi ad ampio raggio gli effetti di questi programmi possono essere modesti se confrontati con programmi che "trattano" un gruppo con un problema specifico. Tuttavia, questi interventi possono produrre cambiamenti in grandi popolazioni (ad es. si pensi ad un programma dedicato alle competenze emotive, oppure alla cittadinanza digitale).
- Prevenzione Selettiva. Un programma dedicato ad un gruppo di studenti in cui il rischio online è presente. In questo caso la presenza del rischio è stata individuata tramite precedenti indagini, segnalazioni fatte dalla scuola, oppure dalla conoscenza della presenza di fattori di rischio in quel determinato territorio. In questi casi gli interventi sono mirati e prevedono programmi formativi strutturati che hanno l'obiettivo di migliorare le competenze digitali e le strategie di problem solving. Può essere un valido programma se si osservano casi in cui la prevenzione universale non ha dato gli esiti previsti.
- Prevenzione Indicata. Un programma di intervento sul caso specifico, è quindi pensato e strutturato per adattarsi agli/lle studenti/studentesse con l'obiettivo di ridurre i comportamenti problematici, oppure dare supporto alle vittime. Per la sua natura questo tipo di intervento si avvale di professionalità diverse perché spesso affronta problemi legati alla salute mentale del minore per cui è opportuno coinvolgere anche la famiglia del/lla ragazzo/a.

4.2 - Cyberbullismo: che cos'è e come prevenirlo

La legge 71/2017 "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo", nell'art. 1, comma 2, definisce il cyberbullismo:

"*qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo*".

La stessa legge e le relative **Linee di orientamento per la prevenzione e il contrasto del cyberbullismo** indicano al mondo scolastico ruoli, responsabilità e azioni utili a prevenire e gestire i casi di cyberbullismo. Le linee prevedono:

- formazione del personale scolastico, prevedendo la partecipazione di un proprio referente per ogni autonomia scolastica;
- sviluppo delle competenze digitali, tra gli obiettivi formativi prioritari (L.107/2015);
- promozione di un ruolo attivo degli studenti (ed ex studenti) in attività di peer education;
- previsione di misure di sostegno e rieducazione dei minori coinvolti;
- Integrazione dei regolamenti e del patto di corresponsabilità con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti;
- Il sistema scolastico deve prevedere azioni preventive ed educative e non solo sanzionatorie.
- **Nomina del Referente per le iniziative di prevenzione e contrasto che:**
    - Ha il compito di coordinare le iniziative di prevenzione e contrasto del cyberbullismo. A tal fine, può avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio.
    - Potrà svolgere un importante compito di supporto al dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d'istituto), atti e documenti (PTOF, PdM, Rav).

Il bullismo online presenta dei tratti caratteristici:

- L'impatto: la diffusione di materiale tramite Internet è incontrollabile e non è

possibile prevederne i limiti (anche se la situazione migliora, video e immagini potrebbero restare online e continuare a diffondersi). Un contenuto offensivo e denigratorio online può, quindi, diventare virale e distruggere in alcuni casi la reputazione della vittima. Nelle situazioni più gravi, le vittime di cyberbullismo si trovano costrette a dover cambiare scuola o addirittura città, ma questo spesso non le aiuta. La Rete, si sa, è ovunque.

- La convinzione dell'anonimato: chi offende online potrebbe tentare di rimanere nascosto dietro un nickname e cercare di non essere identificabile. Sentendosi protetti dall'anonimato ci si sente liberi e più forti nel compiere atti denigratori, senza il timore di essere scoperti. È importante tenere bene a mente, però, che quello dell'anonimato è un "falso mito della Rete". Ogni nostra azione online è, infatti, rintracciabile e riconducibile a noi con gli strumenti opportuni o con l'intervento della Polizia Postale. L'anonimato del cyberbullo, inoltre, è anche uno dei fattori che stanno alla base del forte stress percepito dalla vittima, la quale molte volte non può dare né un nome e né un volto al proprio aggressore;
- L'assenza di confini spaziali: il cyberbullismo può avvenire ovunque, invadendo anche gli spazi personali e privando l'individuo dei suoi spazi-rifugio. La vittima può essere raggiungibile anche a casa e vive nella costante percezione di non avere vie di fuga. Spegnere il cellulare o il computer non basta, così come cancellare tutti i propri profili social. Il solo pensiero che eventuali contenuti denigratori continuino a diffondersi online è doloroso e si accompagna ad un senso costante di rabbia e impotenza.
- L'assenza di limiti temporali: può avvenire a ogni ora del giorno e della notte.
- L'indebolimento dell'empatia: esistono cellule chiamate neuroni specchio che ci permettono di "leggere" gli altri quando li abbiamo di fronte, capirli e di provare emozioni simile a quelle che loro provano, proprio come se fossimo di fronte ad uno specchio. Tale sensazione è data dall'attivazione di una particolare area del cervello. Quando le interazioni avvengono prevalentemente online la funzione speciale di questi neuroni viene meno (mancando la presenza fondamentale dell'altro che è sostituito dal dispositivo). La riduzione di empatia che ne consegue può degenerare nei comportamenti noti messi in atto dai cyberbulli.
- Il feedback non tangibile: il cyberbullo non vede in modo diretto le reazioni della vittima e, ancora una volta, ciò riduce fortemente l'empatia e il riconoscimento del danno provocato.

Per questo il cyberbullo non è mai totalmente consapevole delle conseguenze delle proprie azioni. L'impossibilità di vedere con i propri occhi l'eventuale sofferenza e umiliazione provata dalla vittima fa sì che il tutto venga percepito come "uno scherzo" divertente a cui partecipare, di cui ridere o a cui essere indifferenti. Inoltre, il cyberbullismo non lascia segni fisici evidenti sulla vittima e si consuma in un contesto virtuale che spesso viene percepito dai ragazzi come non "reale", come un mondo ludico a sé stante.
A ciò si aggiungono altre convinzioni o tendenze frequenti nell'uso della Rete sia da parte dei giovani che degli adulti:

- Percezione che online non ci siano norme sociali da rispettare: fra i giovani spesso vige la falsa convinzione secondo cui la Rete sia uno spazio virtuale lontano dalla realtà, in cui vige libertà assoluta e in cui regole e norme sociali della vita quotidiana non valgono;
- La sperimentazione online di identità e personalità multiple: la Rete è per i minori il luogo virtuale per eccellenza in cui mettersi in gioco "fingendo di essere ciò che non si è" per il semplice gusto di sperimentare nuove forme di identità e comportamento;
- Il contesto virtuale come un luogo di simulazione e giochi di ruolo: "la vita sullo schermo" e tutti i comportamenti messi in atto online vengono percepiti solo come un gioco.
- Diffusione di responsabilità: tutti quelli che partecipano anche solo con un like o un commento diventano, di fatto, corresponsabili delle azioni del cyberbullo facendo accrescere la portata dell'azione; mettere un "like" su un social network commentare o condividere una foto o un video che prende di mira qualcuno o semplicemente tacere pur sapendo, mette ragazzi e ragazze nella condizione di avere una responsabilità.

È possibile suddividere gli atti di cyberbullismo in due grandi gruppi:

- **cyberbullismo diretto**: il bullo utilizza strumenti di messaggistica istantanea (es. sms, mms) che hanno un effetto immediato sulla vittima, poiché diretti esclusivamente a lei.
- **cyberbullismo indiretto**: il bullo fa uso di spazi pubblici della Rete (es. social network, blog, forum) per diffondere contenuti dannosi e diffamatori per la vittima. Tali contenuti possono diventare virali e quindi più pericolosi per la vittima anche da un punto di vista psicologico.

È molto importante sottolineare come il cyberbullismo non sia una problematica che riguarda unicamente vittima e cyberbullo. **È un fenomeno sociale e di gruppo.**

La potenziale vittima di cyberbullismo può:

- Apparire nervosa quando riceve un messaggio o una notifica;
- Sembrare a disagio nell'andare a scuola o finge di essere malata (ha spesso mal di stomaco o mal di testa);
- Cambiare comportamento ed atteggiamento in modo repentino;
- Mostrare ritrosia nel dare informazioni su ciò che fa online;
- Soprattutto dopo essere stata online, mostrare rabbia o sentirsi depressa;
- Iniziare ad utilizzare sempre meno Pc e telefono (arrivando ad evitarli);
- Perdere interesse per le attività familiari o per le attività extra-scolastiche che prima svolgeva;
- Il suo rendimento scolastico peggiora.

Nella consapevolezza che le azioni efficaci siano quelle che ricorrono agli strumenti educativi, rieducativi e di mediazione del conflitto, esistono tuttavia responsabilità da conoscere, la possibilità di commettere reati o danni civili e specifici dispositivi giuridici.
Sempre la Legge 71/2017 introduce un provvedimento di carattere amministrativo per gli autori di atti di cyberbullismo, la procedura di ammonimento da parte del Questore: il minore autore può essere convocato dal Questore e ammonito se ritenuto responsabile delle azioni telematiche (il questore convoca il minore, insieme ad almeno un genitore o a chi esercita la responsabilità genitoriale). Gli effetti dell'ammonimento cessano al compimento della maggiore età.

Chi compie atti di bullismo e cyberbullismo può anche essere responsabile di reati penali e danni civili. Nei casi più gravi, basta la denuncia ad un organo di polizia o all'autorità giudiziaria per attivare un procedimento penale (per es. lesioni gravi, minaccia grave, molestie); negli altri casi, la denuncia deve contenere la richiesta che si proceda penalmente contro l'autore di reato (querela). Per poter avviare un procedimento penale nei confronti di un minore è necessario:

- che abbia almeno compiuto 14 anni;
- che, comunque, anche se maggiore di 14 anni, fosse cosciente e volente al momento del comportamento, cioè in grado di intendere e volere (tale non sarebbe, per esempio, un ragazzo con degli handicap psichici).

L'atto di bullismo può violare sia la legge penale, sia quella civile, quindi può dar vita a due processi, l'uno penale e l'altro civile.

Le responsabilità per atti di bullismo e cyberbullismo compiute dal minorenne possono ricadere anche su:

- i genitori, perché devono educare adeguatamente e vigilare, in maniera adeguata all'età del figlio, cercando di correggerne comportamenti devianti. Questa responsabilità generale persiste anche per gli atti compiuti nei tempi di affidamento alla scuola (culpa in educando).
- gli insegnanti e la scuola: perché nei periodi in cui il minore viene affidato all'Istituzione scolastica il docente è responsabile della vigilanza sulle sue azioni e ha il dovere di impedire comportamenti dannosi verso gli altri/e ragazzi/e, insegnanti e personale scolastico o verso le strutture della scuola stessa. A pagare in primis sarà la scuola, che poi potrà rivalersi sul singolo insegnante. La responsabilità si estende anche a viaggi, gite scolastiche, manifestazioni sportive organizzate dalla scuola (culpa in vigilando).
- esiste poi una culpa in organizzando, che si ha quando la scuola non mette in atto le azioni previste per la prevenzione del fenomeno o per affrontarlo al meglio.

Per quanto riguarda la **necessità di segnalazione e rimozione**, 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 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. Il Garante ha pubblicato nel proprio sito il modello per la segnalazione/reclamo in materia di cyberbullismo da inviare a: cyberbullismo@gpdp.it.
Parallelamente, nel caso in cui si ipotizzi che ci si possa trovare di fronte ad una fattispecie di reato (come, ad esempio, il furto di identità o la persistenza di una condotta persecutoria che mette seriamente a rischio il benessere psicofisico del bambino/a o adolescente coinvolto/a in qualità di vittima) si potrà far riferimento agli uffici preposti delle Forze di Polizia per inoltrare la segnalazione o denuncia/querela e permettere alle autorità competenti l'approfondimento della situazione da un punto di vista investigativo. È in tal senso possibile far riferimento a queste tipologie di uffici: Polizia di Stato – Compartimento di Polizia postale e delle Comunicazioni; Questura o Commissariato di P.S. del territorio di competenza; Arma dei Carabinieri – Comando Provinciale o Stazione del territorio di competenza; Polizia di Stato – Commissariato on line (attraverso il portale http:// www.commissariatodips.it).
Per un consiglio e un supporto è possibile rivolgersi alla Helpline di Telefono Azzurro per Generazioni Connesse (1.96.96).

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.

Il nostro Istituto prevede nel proprio curricolo educativo una serie di percorsi strutturati per educare a contrastare
il discorso d'odio. Questi percorsi utilizzano ad esempio video e materiale informativo di Generazioni Connesse ma anche percorsi e attività laboratoriali del Centro Zafira comprensivi di schede per il monitoraggio e valutazine delle attività svolte.

Questi percorsi sono svolti durante le ore dedicate all'educazione civica e sono parte integrante delle attività curricolari.

4.4 - Dipendenza da Internet e gioco online

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

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

La prevenzione passa prima di tutto attraverso la conoscenza del fenomeno da parte non solo della scuola ma anche da parte delle famiglie che spesso non si rendono conto di quanto tempo spendono i figli/e su internet o minimizzano il problema.

La scuola prevede percorsi di formazione (come quello di Generazioni Connesse) per le famiglie e dà ampia diffusione di questi percorsi e degli incontri annuali organizzati in presenza con tutti i genitori dell'Istituto interessati con figure esperte.La S.I.I.Pa.C., la Società Italiana Intervento Patologie Compulsive, definisce la dipendenza da Internet come progressivo e totale assorbimento del soggetto alla Rete.

I segnali patologici di questo che viene descritto come "un vero e proprio abuso della tecnologia", anche denominato "Internet Addiction Disorder" , sono specifici così come

accade per le altre dipendenze più “tradizionali”:

- Dominanza. L’attività domina i pensieri ed il comportamento del soggetto, assumendo un valore primario tra tutti gli interessi.
- Alterazioni del tono dell’umore. L’inizio dell’attività provoca cambiamenti nel tono dell’umore. Il soggetto prova un aumento d’eccitazione o maggiore rilassatezza come diretta conseguenza dell’incontro con l’oggetto della dipendenza.
- Conflitto. Conflitti inter-personali tra il soggetto e coloro che gli sono vicini, conflitti intra-personali interni a se stesso, a causa del comportamento dipendente.
- Ricaduta. Tendenza a ricominciare l’attività dopo averla interrotta.

La tecnologia infatti ha modificato gli ambienti che viviamo e ha un impatto sulla qualità della vita. Gli elementi che contribuiscono al benessere digitale sono:

- la ricerca di equilibrio nelle relazioni anche online
- l’uso degli strumenti digitali per il raggiungimento di obiettivi personali
- la capacità di interagire negli ambienti digitali in modo sicuro e responsabile
- la capacità di gestire il sovraccarico informativo e le distrazioni (ad esempio, le notifiche)

Si tratta di un argomento trasversale. Se ne può parlare quando si parla di cittadinanza digitale, di cyberbullismo, di uso integrativo e non sostitutivo dei dispositivi e della Rete; tanto più può essere utile dedicare al tema un momento specifico e riflettere con studenti e studentesse per fare in modo che la tecnologia sia strumento per raggiungere i propri obiettivi e non sia solo distrazione o addirittura ostacolo.
Anche integrando la tecnologia nella didattica la scuola può insegnare molto, mostrando un suo utilizzo funzionale che possa rendere più consapevoli i ragazzi e le ragazze delle proprie abitudini online.
Si potrebbe riflettere insieme su: come trascorri il tempo on line? Quando aggiunge valore alla tua vita e quando ti fa perdere tempo? Quale atteggiamento potrei cambiare quando sono online? Che ruolo ha e deve avere la tecnologia (internet o il gioco) nella mia vita?
Allo stesso modo quando parliamo di videogiochi, dobbiamo pensarli non in termini negativi ma di benessere digitale. Sono parte del mondo di studenti e studentesse. E, allora, riflettiamo insieme a ragazzi e ragazze su: quando sono una risorsa? Accedono a contenuti adeguati all’età? A che ora e per quanto tempo li usano? Diventa utile riflettere con i ragazzi e le ragazze rispetto all’uso della tecnologia in termini di qualità e tempo.
E' importante far capire che se controlliamo la tecnologia possiamo usarne il pieno potenziale e trarne vantaggi.
E' importante strutturare regole condivise e stipulare con gli alunni/e una sorta di “patto” d’aula e, infine, proporre delle alternative metodologiche e didattiche valide che abbiano come strumento giochi virtuali d’aula (Es. adoperando la LIM o il

dispositivo personale). **È importante, quindi, non demonizzare la tecnologia o il gioco, ma cercare di entrare nel mondo degli/lle studenti e delle studentesse, stabilendo chiare e semplici regole di utilizzo.**

4.5 - Sexting

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

Tra le caratteristiche del fenomeno vi sono principalmente:

- la fiducia tradita: chi produce e invia contenuti sessualmente espliciti ripone fiducia nel destinatario, credendo, inoltre, alla motivazione della richiesta (es. prova d'amore richiesta all'interno di una relazione sentimentale);
- la pervasività con cui si diffondono i contenuti: in pochi istanti e attraverso una condivisione che diventa virale, il contenuto a connotazione sessuale esplicita può essere diffuso a un numero esponenziale e infinito di persone e ad altrettante piattaforme differenti. Il contenuto, così, diventa facilmente modificabile, scaricabile e condivisibile e la sua trasmissione è incontrollabile;
- la persistenza del fenomeno: il materiale pubblicato online può permanervi per un tempo illimitato e potrebbe non essere mai definitivamente rimosso. Un contenuto ricevuto, infatti, può essere salvato, a sua volta re-inoltrato oppure condiviso su piattaforme diverse da quelle originarie e/o in epoche successive.
- La consapevolezza, o comunque la sola idea di diffusione di contenuti personali, si replica nel tempo e può finire con il danneggiare, sia in termini psicologici che sociali, sia il ragazzo/la ragazza soggetto della foto/del video che colui/coloro che hanno contribuito a diffonderla. Due agiti, quindi, che sono fra loro strettamente legati e che rappresentano veri e propri comportamenti criminali i quali hanno ripercussioni negative sulla vittima in termini di autostima, di credibilità, di reputazione sociale off e on line. A ciò si associano altri comportamenti a rischio, di tipo sessuale ma anche riferibili ad abuso di sostanze o di alcool.

I rischi del sexting, legati al revenge porn, possono contemplare: violenza psicosessuale, umiliazione, bullismo, cyberbullismo, molestie, stress emotivo che si riversa anche sul corpo insieme ad ansia diffusa, sfiducia nell'altro/i e depressione.

Il fenomeno è in rapida crescita tra gli adolescenti che spesso forniscono come

motivazione quella di "un banale scherzo" a dimostrazione di quanto possano essere sottovalutate le reali conseguenze di tale diffusione. La reazione più diffusa nella maggior parte dei casi è il silenzio: più della metà delle vittime ha fatto finta di niente e molti non hanno detto nulla per non essere giudicati.

Fondamentali sono tutte le attività di prevenzione che migliorino la conoscenza e consapevolezza dei pericoli della rete e tutte quelle attività che mirano ad aumentare l'autostima ed il rispetto verso se stessi e gli altri.

4.6 - Adescamento online

Il ***grooming*** (dall'inglese "groom" - curare, prendersi cura) rappresenta una tecnica di manipolazione psicologica che gli adulti potenziali abusanti utilizzano per indurre i bambini/e o adolescenti a superare le resistenze emotive e instaurare una relazione intima e/o sessualizzata. Gli adulti interessati sessualmente a bambini/e e adolescenti utilizzano spesso anche gli strumenti messi a disposizione dalla Rete per entrare in contatto con loro.

I luoghi virtuali in cui si sviluppano più frequentemente tali dinamiche sono le chat, anche quelle interne ai giochi online, i social network in generale, le varie app di instant messaging (whatsapp, telegram etc.), i siti e le app di ***teen dating*** (siti di incontri per adolescenti). Un'eventuale relazione sessuale può avvenire, invece, attraverso webcam o live streaming e portare anche ad incontri dal vivo. In questi casi si parla di adescamento o grooming online.

In Italia l'adescamento si configura come reato dal 2012 (art. 609-undecies – l'adescamento di minorenni) quando è stata ratificata la Convenzione di Lanzarote (legge 172 del 1° ottobre 2012).

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere per prevenire ed affrontare la delicata problematica dell'adescamento.

Il 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 e pronti ad affrontare eventuali situazioni a rischio, imparando innanzitutto a gestire le proprie emozioni, il rapporto con il proprio corpo e con gli altri.

Il nostro Istituto promuove da anni per i ragazzi/e delle classi terze della scuola secondaria di primo grado un percorso di Educazione all'affettività con l'aiuto del consultorio locale (progetto EAS). Lo scorso anno è stato chiesto di poter estendere il

progetto anche alle classi prime e seconde.

Ogni anno sono organizzati incontri informativi con la Polizia di Stato per meglio informare i ragazzi sui pericoli e le responsabiità.

È molto importante, inoltre, che ragazzi e ragazze sappiano a chi rivolgersi in caso di problemi, anche quando pensano di aver fatto un errore, si vergognano o si sentono in colpa. Gli adulti coinvolti, genitori e docenti, devono essere un punto di riferimento per il minore che deve potersi fidare di loro e non sentirsi mai giudicato, ma compreso e ascoltato. Affinché ciò avvenga è necessario tenere sempre aperto un canale di comunicazione con loro sui temi dell'affettività, del digitale e perché no, della sessualità. Oltre agli insegnanti di classe ed i componenti del team anti-bullismo, un ruolo fondamentale lo svolgono quindi le famiglie ed i compagni/gli amici che spesso segnalano prima delle vittime stesse.

Nel nostro Istituto è prevista una mail ed una cassetta per le segnalazioni di bullismo-cyberbullismo e altre problematiche ed ogni anno viene attivato uno sportello d'ascolto a cui sempre più studenti si stanno rivolgendo.

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.

Nel contrastare la diffusione della pedopornografia risulta utilissima l'attività educativa sull'affettività e le relazioni, sottolineando sempre la necessità di rivolgersi ad un adulto quando qualcosa online mette a disagio.

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, anche attraverso la promozione dei servizi delle hotline o al Vademecum di Generazioni Connesse.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2023/2024).

Scegliere almeno 1 di queste azioni:

x Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli

studenti/studentesse.

x 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.

x 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.

x 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.

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

x 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.

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

x 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.

x 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:

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

x 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.

x 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.

x 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.

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

x 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.

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

x 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.

x 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 intervento che i Dirigenti Scolastici sono chiamati a effettuare, qualora vengono a conoscenza di episodi di bullismo o cyberbullismo, sono integrate e previste nel Regolamento di Istituto e nel Patto di Corresponsabilità, al fine di regolamentare l'insieme dei provvedimenti sia di natura disciplinare sia di natura educativa e di prevenzione.

Intervenire in situazioni di bullismo o cyberbullismo implica una conoscenza del fenomeno, la capacità di agire, attraverso l'utilizzo di strategie e interventi mirati e l'abilità di prevenire, attraverso attività educative in grado di rafforzare le dinamiche relazionali e le competenze emotive.

A tal proposito la Scuola ha attivato il Team Antibullismo e per le Emergenze che include docenti formati nel Corso di Formazione "Prevenzione e contrasto al bullismo, cyberbullismo e dipendenza da internet" organizzato dalla Piattaforma ELISA e Università di Firenze.

La Scuola, non potendo intervenire direttamente sui telefoni cellulari degli alunni senza autorizzazione dei genitori, ha il dovere di monitorare le attività svolte al suo interno attraverso i dispositivi digitali; ogni docente ha il dovere di segnalare la presenza su un dispositivo in dotazione alla scuola dei seguenti contenuti:

- Dati sensibili o riservati (foto, immagini, video personali, informazioni private proprie o di amici, l’indirizzo di casa o il telefono, ecc.);
- Contenuti che possano considerarsi in qualche modo lesivi dell’immagine altrui (commenti offensivi, minacce, osservazioni diffamatorie o discriminatorie, foto o video denigratori, videogiochi che contengano un’istigazione alla violenza, ecc.);
- Contenuti riconducibili alla sfera sessuale: messaggi, immagini o video a sfondo sessuale, come foto di nudo o semi-nudo.

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.

Il Personale Scolastico, dinanzi al sospetto o alla 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.

In questa sezione del documento vengono inserite le procedure standardizzate per la segnalazione e gestione dei problemi connessi a comportamenti online a rischio di studenti e studentesse condivise sul sito di "Generazioni connesse" con l'unica modifica consistente nell'informare e coinvolgere sempre la famiglia.

Per quanto riguarda la gestione dei casi, il Nostro Istituto ha individuato un Referente contro il Bullismo e il Cyberbullismo e un Team antibullismo costituito da quattro

membri, rappresentanti i tre ordini scolastici e i plessi facente parte dell'Istituto.

La segnalazione del caso dovrà essere fatta dal personale scolastico attraverso la compilazione della "Scheda di prima segnalazione" (vedi allegato 1) fornita dalla piattaforma Elisa e personalizzata dal nostro Team, pubblicate sul sito della Scuola in una specifica sezione a disposizione di studenti, familiari, docenti e personale scolastico. La "Scheda di prima segnalazione" va inviata via mail al team antibullismo che, in breve tempo, dopo un ulteriore confronto con il Consiglio di Classe e il Team, provvede a compilare la "Scheda di valutazione approfondita" (vedi allegato 2). La suddetta scheda permetterà ai membri del Team antibullismo, attraverso l'inserimento di specifiche informazioni, di individuare il codice di gravità sia riferito alla vittima sia al bullo. In base alle informazioni acquisite dalle diverse sezioni si delinea come livello di priorità dell'intervento e il coinvolgimento di specifiche figure:

- Codice verde: l'intervento è di competenza del docente di Classe con il coinvolgimento del Consiglio di Classe e della famiglia; il docente può essere assistito da uno dei membri del Team antibullismo;
- Codice giallo: interventi indicati e strutturati sia a scuola sia individualmente, con il coinvolgimento della rete se non ci sono risultati. E' sempre previsto il coinvolgimento della famiglia sia del bullo che della vittima.
- Codice rosso: interventi di emergenza con il supporto della rete e di specifiche figure; coinvolgimento del Dirigente Scolastico. E' sempre previsto il coinvolgimento della famiglia sia del bullo che della vittima.

Il Referente contro il Bullismo e il Cyberbullismo dovrà essere informato, dai membri del team, di ogni singola segnalazione e a lui perverranno le schede di valutazione approfondita.

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.

La scuola ha individuato le figure che costituiscono un team preposto alla gestione della segnalazione: Referente contro il Bullismo e il Cyberbullismo e un Team antibullismo costituito da quattro membri, rappresentanti i tre ordini scolastici e i plessi facente parte dell'Istituto.

Nell'affrontare i casi, si prevede la collaborazione con figure esterne, 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.

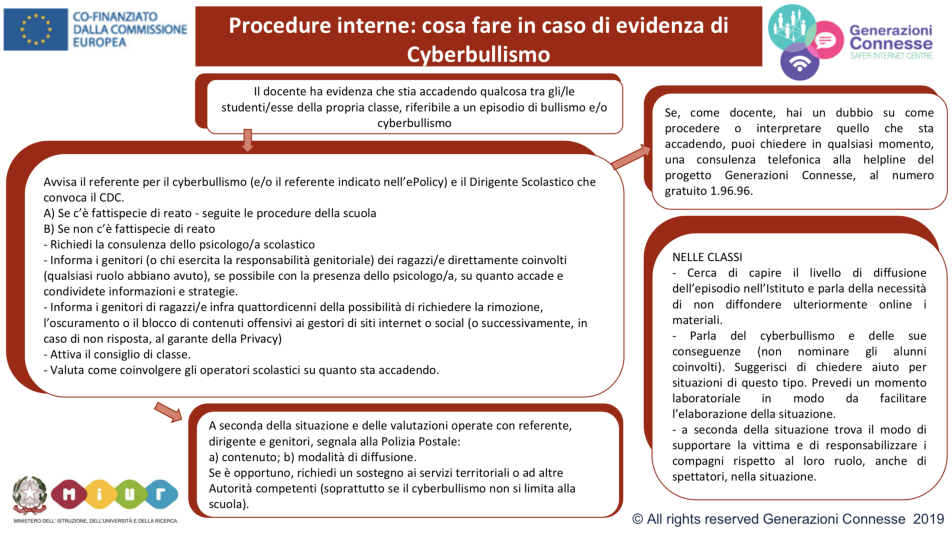
La Nostra Scuola si impegna a collaborare con i principali Servizi e le Agenzie del territorio:

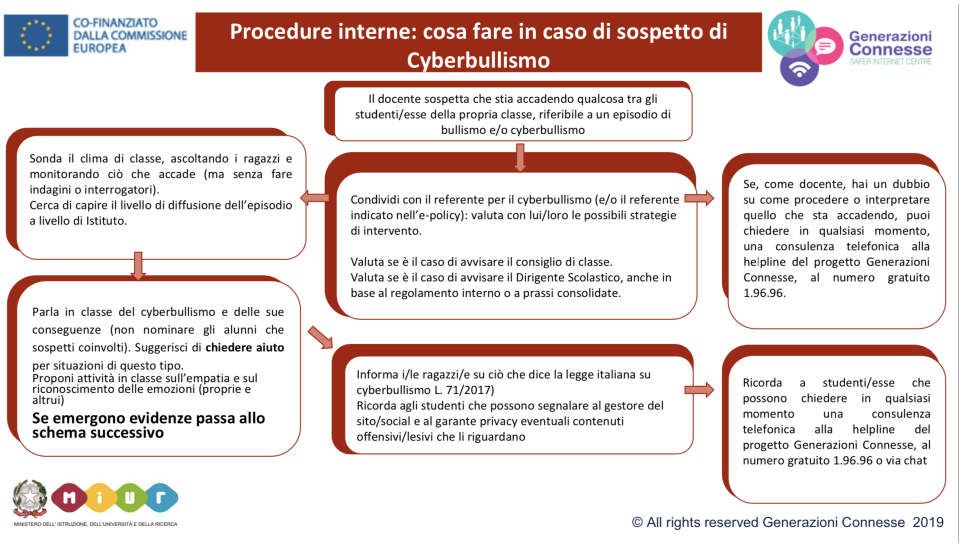
- ASL Roma 6 con la partecipazione al Progetto SPS "Scuole che Promuovono la Salute"
- il Progetto Scuola Attiva che ingloba docenti formati nel Corso di Formazione "Prevenzione e contrasto al bullismo, cyberbullismo e dipendenza da internet"

- Incontri con gli esperti dell'Ambulatorio contro le Dipendenze del Policlinico Gemelli di Roma;
- Sportello di ascolto psicologico per docenti, alunni e genitori;
- Collaborazione con il Consultorio familiare del territorio per progetti sull'affettività e sessualità
- Polizia Postale e delle Comunicazioni
- Servizi Sociali del Territorio
- Forze dell'ordine
- Help Desk

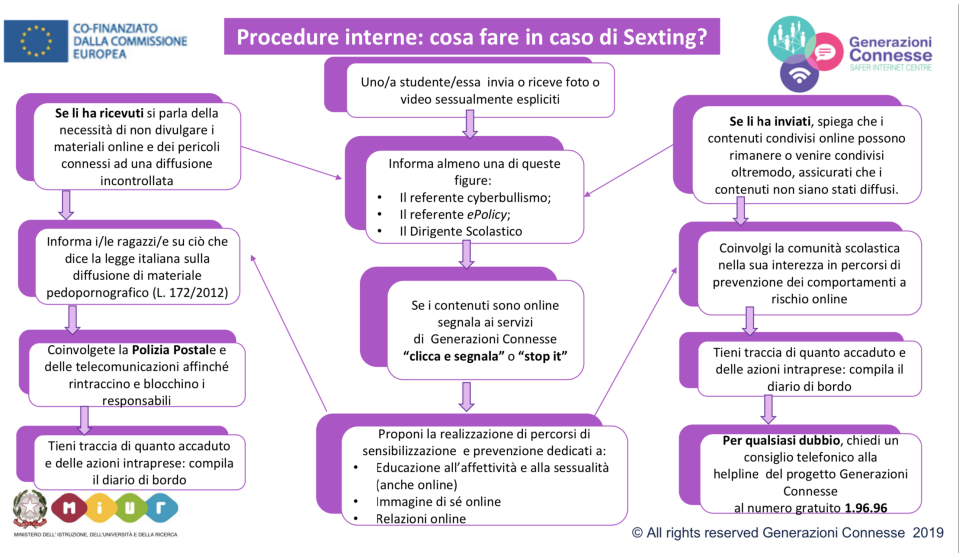
5.4. - Allegati con le procedure

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

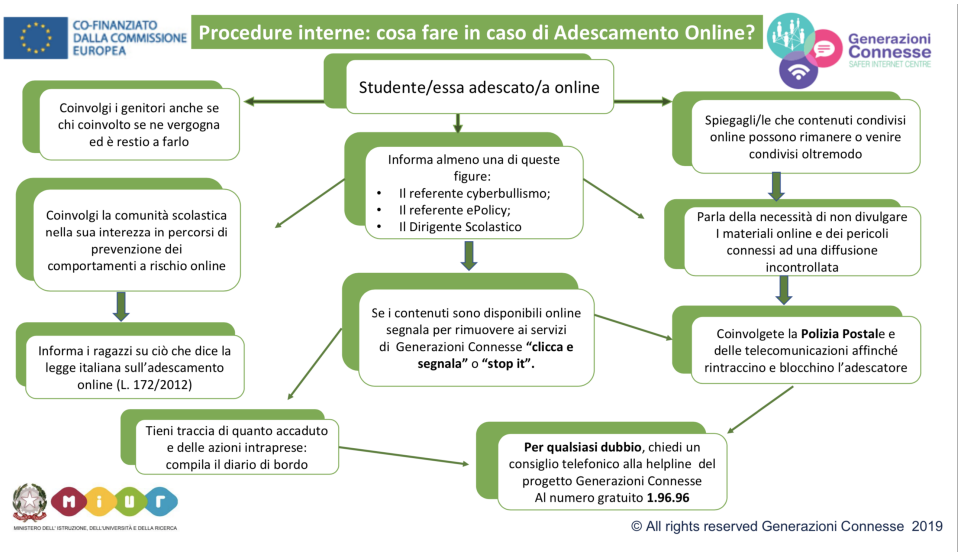




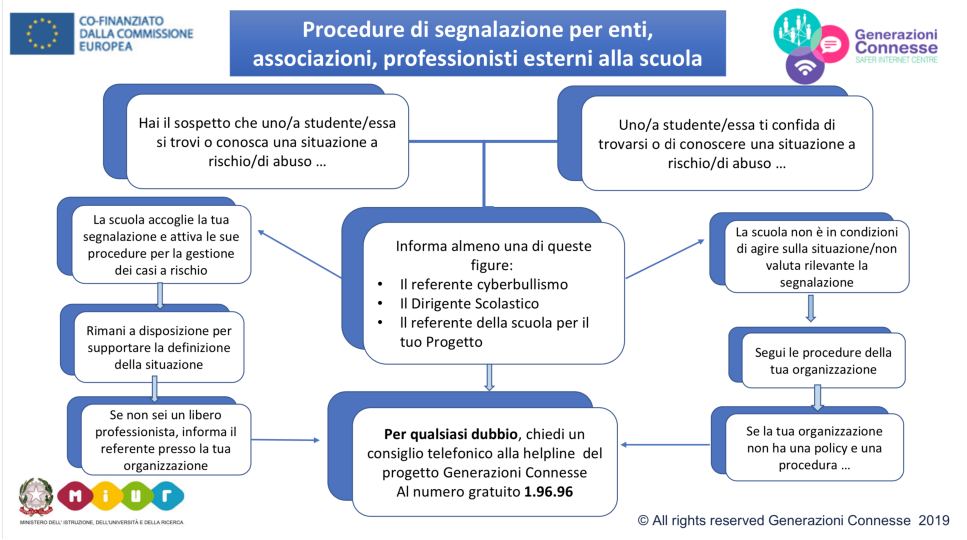
Procedure interne: cosa fare in caso di sexting?



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

Definizione delle azioni da intraprendere a seconda della specifica del caso

Si definisce bullismo *"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 online 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" (L.71/2017 Art. 1- Comma 2).*

Quando ci si trova dinanzi ad un caso (Di evidenza o di sospetto) di cyberbullismo (denunciato dalla vittima stessa, da persone vicino alla vittima o scoperto da un docente) si dovrà procedere nel seguente modo:

- Il docente venuto a conoscenza del fatto dovrà:

- Informare tempestivamente il Team antibullismo con la compilazione e l'invio della "scheda di prima segnalazione" al canale predisposto;

- Informare tempestivamente il Consiglio di Classe dell'alunno oggetto di cyberbullismo e rendersi disponibile ad un ulteriore confronto con il Referente e i membri del Team antibullismo per la compilazione della "Scheda di valutazione approfondita"

- Informare la famiglia dell'alunno oggetto di cyberbullismo;

- Il Referente, in collaborazione con il Consiglio di Classe, raccoglierà tutte le informazioni possibili, informazioni che gli permetteranno di individuare il codice di gravità e di conseguenza la priorità dell'intervento e il coinvolgimento di specifiche figure;

- Il Consiglio di classe:

- Valuterà, a seconda della gravità del caso, come sanzionare il/i responsabili (qualora sia stato possibile individuarli);

- Il Dirigente valuterà se la segnalazione debba essere rivolta ad organi esterni alla Scuola.

Casi di sexting

Con il termine *sexting* s'intende l'invio e/o la ricezione di contenuti (video o immagini) sessualmente espliciti che ritraggono se stessi o gli altri.

Qualora ci si trovi di fronte ad un caso di sexting (denunciato dalla vittima stessa, da persone vicino alla vittima o scoperto da un docente) si procederà in maniera analoga ai casi di cyberbullismo.

Casi di adescamento online o grooming 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.

Qualora ci si trovi di fronte ad un caso di sexting (denunciato dalla vittima stessa, da persone vicino alla vittima o scoperto da un docente) si procederà in maniera analoga ai casi di cyberbullismo.

Il nostro piano d'azioni

GIUSEPPE DI VICO
23.11.2023
11:58:52
GMT+00:00