Documento di ePolicy

CSIC8AU004

IC PRAIA A MARE

VIA VERDI 40 - 87028 - PRAIA A MARE - COSENZA (CS)

PATRIZIA GRANATO

Verbale n. 13 del 26/05/2021 Delibera n.96

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.

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.

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.

Scopo del presente documento di e- policy è di informare l'utenza per un uso corretto e responsabile delle apparecchiature informatiche collegate alla rete in dotazione alla Scuola, nel rispetto della normativa vigente. In particolare l'intento della scuola è quello di promuovere l'uso consapevole e critico da parte degli alunni delle tecnologie digitali e di internet, di far acquisire loro procedure e competenze "tecniche" ma anche corrette norme comportamentali, di prevenire ovvero rilevare e
fronteggiare le problematiche che derivano da un utilizzo non responsabile, pericoloso o dannoso, delle tecnologie digitali .
Gli utenti, soprattutto minori, devono essere pienamente consapevoli dei rischi a cui si espongono quando navigano in rete. Di fatto esiste la possibilità che durante il lavoro online si possa entrare accidentalmente in contatto con materiale inadeguato e/o illegale, pertanto la Scuola promuove l'adozione di strategie che limitino l'accesso a siti e/o applicazioni illeciti.
Gli insegnanti hanno la responsabilità di guidare gli studenti nelle attività online a scuola e di indicare regole di condotta chiare per un uso critico e consapevole di Internet anche a casa, per prevenire il verificarsi di situazioni potenzialmente pericolose.

1.2 - Ruoli e responsabilità

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

Dirigente scolastico

Il ruolo del Dirigente scolastico nel promuovere l'uso consentito delle tecnologie e di internet
include i seguenti compiti:

- garantire la sicurezza (tra cui la sicurezza on-line) dei membri della comunità scolastica;
- garantire che tutti gli insegnanti ricevano una formazione adeguata per svolgere efficacemente l'insegnamento volto a promuovere una cultura dell'inclusione, del rispetto dell'altro/a e delle differenze, un utilizzo positivo e responsabile delle Tecnologie dell'Informazione e della comunicazione (TIC);
- garantire l'esistenza di un sistema in grado di consentire il monitoraggio e il controllo interno della sicurezza on-line;
- comprendere e seguire le procedure previste dalle norme in caso di reclami o attribuzione di

responsabilità al personale scolastico in relazione a incidenti occorsi agli alunni nell'utilizzo
delle TIC a scuola.

Animatore digitale

Il ruolo dell'Animatore digitale include i seguenti compiti:

- stimolare la formazione interna all'istituzione negli ambiti di sviluppo della "scuola digitale" e fornire consulenza e informazioni al personale in relazione ai rischi on-line e alle misure di prevenzione e gestione degli stessi;
- monitorare e rilevare le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola, nonché proporre la revisione delle politiche dell'istituzione con l'individuazione di soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola;
- assicurare che gli utenti possano accedere alla rete della scuola solo tramite password personali applicate e regolarmente cambiate e curare la manutenzione e lo sviluppo del sito web della scuola per scopi istituzionali e consentiti (istruzione e formazione);

Referente Cyberbullismo d'Istituto:

- Coordina iniziative di prevenzione e contrasto del cyberbullismo messe in atto dalla scuola;
- Predispone un documento di rilevazione di incidenti di sicurezza in rete;
- Coordina il Team di Emergenza;
- Promuove attività di Formazione interna per la diffusione di norme per l'uso corretto delle tecnologie al corpo docente e genitori.
- Attività di prevenzione per gli alunni ;
- Partecipazione ad iniziative promosse dal MIUR/USR.

Direttore dei servizi generali e amministrativi

Il ruolo del direttore dei servizi generali e amministrativi include i seguenti compiti:

- assicurare, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per garantire che l'infrastruttura tecnica della scuola sia funzionante, sicura e non aperta a uso improprioo a dannosi attacchi esterni;
- garantire il funzionamento dei diversi canali di comunicazione della scuola (sportello,circolari, sito web, ecc.) all'interno della scuola e fra la scuola e le famiglie degli alunni per la notifica di documenti e informazioni del Dirigente scolastico e dell'Animatore digitale nell'ambito dell'utilizzo delle tecnologie digitali e di internet.

Docenti

Il ruolo del personale docente e di ogni figura educativa che lo affianca include i seguenti compiti:

- informarsi/aggiornarsi sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di internet e sulla politica di sicurezza adottata dalla scuola,
- garantire che le modalità di utilizzo corretto e sicuro delle TIC e di internet siano integrate nel curriculum di studio e nelle attività didattiche ed educative delle classi;
- garantire che gli alunni capiscano e seguano le regole per prevenire e contrastare l'utilizzo scorretto e pericoloso delle TIC e di internet rispettandone il regolamento;
- assicurare che gli alunni abbiano una buona comprensione delle opportunità di ricerca offerte dalle tecnologie digitali e dalla rete ma anche della necessità di evitare il plagio e di rispettare la normativa sul diritto d'autore;
- assicurare la riservatezza dei dati personali trattati ai sensi della normativa vigente;
- nelle lezioni in cui è programmato l'utilizzo di Internet, guidare gli alunni a siti controllati e
  verificati come adatti per il loro uso e controllare che nelle ricerche su Internet siano trovati e trattati solo materiali idonei;
- comunicare al Referente Bullismo e Cyberbullismo d'Istituto e ai genitori difficoltà, bisogni o disagi espressi dagli alunni(ovvero valutazioni sulla condotta non adeguata degli stessi)rilevati a scuola e connessi all'utilizzo delle TIC, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo;
- segnalare al Dirigente scolastico e ai genitori qualsiasi abuso rilevato a scuola nei confronti degli alunni in relazione all'utilizzo delle tecnologie digitali o di internet, per l'adozione delle procedure previste dalle norme.

Alunni

Il ruolo degli alunni include i seguenti compiti:

- essere responsabili, in relazione al proprio grado di maturità e di apprendimento, per l'utilizzo dei sistemi delle tecnologie digitali in conformità con quanto richiesto dai docenti;
- avere una buona comprensione delle potenzialità offerte dalle TIC per la ricerca di contenuti e materiali ma anche della necessità di evitare il plagio e rispettare i diritti d'autore;
- comprendere l'importanza di adottare buone pratiche di sicurezza on-line quando si utilizzano le tecnologie digitali per non correre rischi;
- adottare condotte rispettose degli altri anche quando si comunica in rete;
- esprimere domande o difficoltà o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o di internet ai docenti e ai genitori.

Genitori

Il ruolo dei genitori degli alunni include i seguenti compiti:

- Sostenere la linea di condotta della scuola adottata nei confronti dell'utilizzo delle tecnologie dell'Informazione e delle Comunicazioni nella didattica;
- Seguire gli alunni nello studio a casa adottando i suggerimenti e le condizioni d'uso delle TIC indicate dai docenti, in particolare controllare l'utilizzo del pc e di internet
- Concordare con i docenti linee di intervento coerenti e di carattere educativo in relazione aiproblemi rilevati per un uso non responsabile o pericoloso delle tecnologie digitali o di internet;
- Fissare delle regole per l'utilizzo del computer e tenere sotto controllo l'uso che i figli fanno di internet e del telefonino in generale.

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).

Dotarsi di un'informativa sintetica sull'ePolicy comprensiva delle procedure di segnalazione da condividere con tutte le figure che operano con studenti e studentesse, significa non solo tutelare questi ultimi e la scuola stessa, ma anche porre in essere nuove modalità per rilevare, limitare e contrastare possibili pericoli legati a

condotte educative non professionali. Tale documento dovrà chiarire il sistema di azioni e le procedure di segnalazione da seguire valide anche per i professionisti e le organizzazioni esterne, finalizzate a rilevare e gestire le problematiche connesse ad un uso non consapevole delle tecnologie digitali.

In questo modo, si facilita la presa in carico da parte della scuola, qualora si verificassero problematiche derivanti da un utilizzo non corretto delle tecnologie digitali o quando, nei casi più estremi, si sospettassero forme di maltrattamento/abuso sia nel reale che nel virtuale, sia di tipo fisico che psicologico a danno di minori. Tale documento, inoltre, permette di tutelare ragazzi e ragazze da comportamenti potenzialmente rischiosi messi in atto da soggetti esterni alla scuola e che si trovano ad operare all'interno dell'Istituto.

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.

Come condividere e comunicare la politica di e-safety agli alunni.

- Tutti gli alunni saranno informati che la rete, l'uso di Internet e di ogni

dispositivo digitale saranno controllati dagli insegnanti e utilizzati solo con la loro autorizzazione.
- L'istruzione degli alunni riguardo all'uso responsabile e sicuro di internet precederà l'accesso alla rete;
- L'elenco delle regole per la sicurezza on-line sarà pubblicato in tutte le aule o laboratori con accesso a internet;
- Sarà data particolare attenzione nell'educazione sulla sicurezza agli aspetti per i quali gli
alunni risultano più esposti o rispetto ai quali risultano più vulnerabili".

Condividere e comunicare la politica di e-safety al personale

La linea di condotta della scuola in materia di sicurezza nell'utilizzo delle tecnologie digitali e di internet sarà discussa negli organi collegiali e comunicata formalmente a tutto il personale con il presente documento e altro materiale informativo anche sul sito web;

Per proteggere tutto il personale e gli alunni, la scuola metterà in atto una linea di condotta di utilizzo accettabile, controllato e limitato alle esigenze didattiche essenziali:

- Il personale docente sarà reso consapevole del fatto che il traffico in internet può essere monitorato e si potrà risalire al singolo utente registrato;
- Un'adeguata informazione/formazione on-line del personale docente nell'uso sicuro e responsabile di internet, sia professionalmente che personalmente, sarà fornita a tutto il personale, anche attraverso il sito web della scuola;
- Il sistema di filtraggio adottato e il monitoraggio sull'utilizzo delle TIC sarà supervisionato dall'Animatore digitale, che segnalerà al DSGA eventuali problemi che dovessero richiedere acquisti o interventi di tecnici;

Condividere e comunicare la politica di e-safety ai genitori

- L'attenzione dei genitori sulla sicurezza nell'uso delle tecnologie digitali e di internet sarà attirata nelle news o in altre aree del sito web della scuola;
- Sarà incoraggiato un approccio di collaborazione nel perseguimento della sicurezza nell'uso delle TIC e di internet in occasione degli incontri scuola-famiglia, assembleari, collegiali e individuali;
- L'Animatore digitale fornirà ai genitori suggerimenti e indicazioni per l'uso sicuro delle tecnologie digitali e di internet anche a casa;
- L'Animatore digitale e i docenti di classe forniranno ai genitori indirizzi sul web relativi a risorse utili per lo studio e a siti idonei ed educativi per gli alunni, sistemi di filtraggio e attività educative per il tempo libero.

1.5 - Gestione delle infrazioni alla ePolicy

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.

Gestione delle infrazioni alla Policy.

Disciplina degli alunni

Le potenziali infrazioni in cui è possibile che gli alunni incorrano a scuola nell'utilizzo delle tecnologie digitali di internet di cui si dispone per la didattica, in relazione alla fascia di età considerate, sono prevedibilmente le seguenti:

- un uso della rete per giudicare, infastidire o impedire a qualcuno di esprimersi o partecipare;
- l'invio incauto o senza permesso di foto o di altri dati personali come l'indirizzo di casa o il telefono;
- la condivisione di immagini intime o troppo spinte;
- la comunicazione incauta e senza permesso con sconosciuti;
- il collegamento a siti web non indicati dai docenti. Gli interventi correttivi previsti per gli alunni sono rapportati all'età e al livello di sviluppo dell'alunno. Infatti più gli alunni sono piccoli, più i comportamenti "da correggere" sono dovuti a uno sviluppo cognitivo, affettivo e morale incompleto o a fasi critiche transitorie, che devono essere compresi e orientati proprio dagli educatori, nella prospettiva del raggiungimento di una maggiore consapevolezza e maturità da parte dell'alunno.

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

- il richiamo verbale;
- il richiamo verbale con particolari conseguenze (riduzione o sospensione dell'attività gratificante);
- il richiamo scritto con annotazione sul diario;
- Nota informativa ai genitori o tutori mediante registro elettronico.
- la convocazione dei genitori da parte degli insegnanti;
- la convocazione dei genitori da parte del Dirigente scolastico.
- Intervento dello Psicologo della Scuola (Sprtello d'ascolto)

Contestualmente sono previsti interventi di carattere educativo di rinforzo dei comportamenti corretti e riparativi dei disagi causati, di ri-definizione delle regole sociali di convivenza attraverso la
partecipazione consapevole e attiva degli alunni della classe, di prevenzione e gestione positiva dei conflitti, di moderazione dell'eccessiva competitività, di promozione di

rapporti amicali e di reti di solidarietà, di promozione della conoscenza e della gestione delle emozioni.

Disciplina del personale scolastico

Le potenziali infrazioni in cui è possibile che il personale scolastico e in particolare i docenti incorrano nell'utilizzo delle tecnologie digitali e di internet sono diverse e alcune possono
determinare, favorire o avere conseguenze di maggiore o minore rilievo sull'uso corretto e responsabile delle TIC da parte degli alunni:

- un utilizzo delle tecnologie e dei servizi della scuola, d'uso comune con gli alunni, non connesso alle attività di insegnamento o al profilo professionale, anche tramite 'installazione di software o il salvataggio di materiali non idonei;
- un utilizzo delle comunicazioni elettroniche con i genitori e gli alunni non compatibile con il ruolo professionale.
- un trattamento dei dati personali, comuni e sensibili degli alunni, non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi.
- una diffusione delle password assegnate e una custodia non adeguata degli strumenti e degli
  accessi di cui possono approfittare terzi;
- una vigilanza elusa dagli alunni che può favorire un utilizzo non autorizzato delle TIC e possibili
- incidenti.
- insufficienti interventi nelle situazioni critiche di contrasto a terzi, correttivi o di sostegno agli alunni, di segnalazione ai genitori, al Dirigente scolastico, all'Animatore digitale.

Il Dirigente scolastico può controllare l'utilizzo delle TIC per verificarne la conformità alle regole di sicurezza, compreso l'accesso a internet,la posta elettronica inviata/pervenuta a
scuola, procedere alla cancellazione di materiali inadeguati o non autorizzati dal sistema informatico della scuola,conservandone una copia per eventuali successive investigazioni.
Tutto il personale è tenuto a collaborare con il Dirigente Scolastico e a fornire ogni informazione utile per le valutazioni del caso e per l'avvio di procedimenti che possono avere carattere organizzativo gestionale,disciplinare, amministrativo, penale, a seconda del tipo o della gravità delle infrazioni commesse. Le procedure sono quelle previste dalla legge e dai
contratti di lavoro.

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.

La policy richiede l'integrazione con l'inserimento delle seguenti norme:
- Le apparecchiature presenti nella scuola sono un patrimonio comune, quindi, vanno utilizzate con il massimo rispetto.
- Le postazioni informatiche dell'istituto possono essere utilizzati esclusivamente per attività di insegnamento, funzionali all'insegnamento e di formazione del personale docente e non docente.
- In caso di malfunzionamento o guasto dei computer bisogna darne tempestiva segnalazione al responsabile di laboratorio.
- In caso di malfunzionamento non risolvibile dal responsabile di laboratorio, il suddetto contatterà la segreteria o l'Animatore Digitale.

Disposizioni sull'uso dei software

- I software installati sono ad esclusivo uso didattico.
- In base alle leggi che regolano la distribuzione delle licenze, i prodotti software presenti in laboratorio non sono disponibili per il prestito individuale. Nei casi in cui lo fossero in base a precise norme contrattuali i docenti interessati, dopo aver concordato il prestito con il Responsabile di laboratorio, devono compilare l'apposito registro di consegna software custodito in laboratorio.
- E' fatto divieto di usare software non conforme alle leggi sul copyright. E' cura dell'insegnante utente di verificarne la conformità. Gli insegnanti possono installare nuovo software sui PC del laboratorio della propria scuola, previa autorizzazione scritta del DS solo se il software installato rispetta le leggi sul copyright.
- E' responsabilità degli insegnanti che chiedono al Responsabile di laboratorio di effettuare copie di cd/dvd per uso didattico, di assicurarsi che la copia non infranga le leggi sul copyright in vigore

Accesso a internet

- L'accesso a Internet è consentito al personale docente e non docente solo ad esclusivo uso didattico e/o di formazione e alle classi accompagnate e sotto la responsabilità di un insegnante;
- L'utente è direttamente responsabile, civilmente e penalmente, a norma delle vigenti leggi, per

l'uso fatto del servizio Internet;

- E' vietato inserire sui pc connessi in rete programmi contenenti virus, scaricare software non
  autorizzati da internet, scaricare e installare software senza licenza.

Norme finali

Il Responsabile di laboratorio che verifichi un uso del laboratorio contrario a disposizioni di legge o del regolamento interno deve darne comunicazione per iscritto al Dirigente Scolastico.

UTILIZZO DEL TELEFONO CELLULARE E DEI VARI DISPOSITIVI ELETTRONICI DURANTE LE ATTIVITÀ SCOLASTICHE

a) Salvo casi del tutto eccezionali, i telefoni cellulari non devono essere portati a scuola e non devono comunque essere utilizzati durante l'orario scolastico. Se,malgrado il divieto, gli studenti
verranno sorpresi ad usare il cellulare, lo stesso verrà temporaneamente requisito dai docenti che registreranno l'episodio sul registro di classe e, in collaborazione con il personale ausiliario e/o con la segreteria, convocheranno per le vie brevi i genitori interessati ai quali verrà riconsegnato il
cellulare requisito.

Avuto inoltre riguardo per il fatto che i moderni cellulari possono essere utilizzati anche per scattare foto (o effettuare riprese filmate) e per trasferirle sui social, si informano i Sigg. genitori che eventi di questo tipo, se si concretizzano durante l'orario scolastico, si possono configurare anche come reati per i quali non si esclude la segnalazione ai competenti organi di Pubblica Sicurezza.

b) L'Istituzione Scolastica non ha e comunque non si assume alcuna responsabilità né relativamente all'uso improprio o pericoloso che gli studenti dovessero fare del cellulare (es.: inviare/ricevere messaggi a/da soggetti ignoti agli stessi genitori), né relativamente a smarrimenti e/o 'sparizioni'di telefonini cellulari o di lettori mp3 o di hard/disk portatili o pen drive.

c) In ogni caso,i genitori tengano conto che le comunicazioni urgenti ed improcrastinabili possono essere trasmesse ai loro figli durante l'orario scolastico rivolgendosi telefonicamente alle singole sedi scolastiche ovvero in Segreteria.

d) La scuola non pone alcun ostacolo all'utilizzo di cd/dvd rom o di hard - disk portatili come strumenti di lavoro e di studio. Ciò che a riguardo compete alle famiglie è il controllo periodico del
contenuto di questi strumenti per evitare che qualche studente 'trasporti' a scuola immagini / testi / filmati per così dire "sconvenienti" avendoli scaricati.

Per impedire che le stesse postazioni dei laboratori scolastici possano essere

furtivamente utilizzate per visitare siti volgari e pericolosi, la scuola si è da tempo dotata di un software di sicurezza che filtra gli accessi ad internet e protegge
quindi i visitatori meno esperti. Oltre a questo sofisticato sistema di protezione che blocca l'accesso ai siti di cui si discorre, la scuola ovviamente mette in campo soprattutto la vigile attenzione
educativa di ogni singolo docente.

1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

L'E-policy viene aggiornata periodicamente e quando si verificano cambiamenti significativi in riferimento all'uso delle tecnologie digitali all'interno della scuola. Le modifiche del documento saranno discusse con tutti i membri del personale docente. Il monitoraggio del documento sarà realizzato a partire da una valutazione della sua efficacia in riferimento agli obiettivi specifici che lo stesso si pone.

Il referente Bullismo e Cyberbullismo nominato dal Dirigente Scolastico provvede annualmente alla revisione e aggiornamento dell'ePolicy del Regolamento d'Istituto .

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 1 evento di presentazione del progetto Generazioni Connesse rivolto ai docenti
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse 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 3 eventi di presentazione del progetto Generazioni Connesse rivolto agli studenti
- Organizzare 3 eventi di presentazione del progetto Generazioni Connesse rivolto ai docenti
- Organizzare 3 eventi di presentazione del progetto Generazioni Connesse rivolto ai genitori
- Organizzare 3 eventi di presentazione e conoscenza dell'ePolicy rivolto agli studenti
- Organizzare 3 eventi di presentazione e conoscenza dell'ePolicy rivolto ai docenti
- Organizzare 3 eventi di presentazione e conoscenza dell'ePolicy rivolto ai genitori

Capitolo 2 - Formazione e curricolo

2.1. Curricolo sulle competenze digitali per gli studenti

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

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

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

L'impiego corretto e consapevole delle TIC costituisce un fattore di innovazione della didattica e può utilmente contribuire all'aumento della motivazione e del rendimento degli studenti e alla modifica delle pratiche tradizionali di insegnamento: è quindi importante coglierne le potenzialità rispetto a contesti e finalità specifici. Per sostenere questo processo all'interno della scuola è necessario investire sulla formazione e l'aggiornamento degli insegnanti, soprattutto in relazione alla didattica per competenze e all'innovazione metodologico-didattica.

VALUTAZIONE DELLE COMPETENZE CHIAVE EUROPEE

Competenze digitali declinate secondo le **cinque aree** del quadro di riferimento DIGCOMP (Quadro comune di riferimento europeoper le competenze digitali).

1. **INFORMAZIONE**: identificare, localizzare, recuperare, conservare, organizzare e analizzare le informazioni digitali, giudicare la loro importanza e

lo scopo.

2. **COMUNICAZIONE**: comunicare in ambienti digitali, condividere risorse attraverso strumenti on-line, collegarsi con gli altri e collaborare attraverso strumenti digitali, interagire e partecipare alle comunità e alle reti.
3. **CREAZIONE DI CONTENUTI**: creare e modificare nuovi contenuti (da elaborazione testi a immagini e video); integrare e rielaborare le conoscenze e i contenuti; produrre espressioni creative, contenuti media e programmare; conoscere e applicare i diritti di proprietà intellettuale e le licenze
4. **SICUREZZA**: protezione personale, protezione dei dati, protezione dell'identità digitale, misure di sicurezza, uso sicuro e sostenibile.
5. **PROBLEM-SOLVING**: identificare i bisogni e le risorse digitali, prendere decisioni informate sui più appropriati strumenti digitali secondo lo scopo o necessità, risolvere problemi concettuali attraverso i mezzi digitali, utilizzare creativamente le tecnologie, risolvere problemi tecnici, aggiornare la propria competenza e quella altrui.

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

È fondamentale che i docenti tutti siano formati ed aggiornati sull'uso corretto, efficace ed efficiente delle TIC nella didattica, al fine di usarle in modo integrativo ed inclusivo.

Ciò si rende necessario per fornire agli studenti e alle studentesse modelli di utilizzo positivo, critico e specifico delle nuove tecnologie e per armonizzare gli apprendimenti.

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

Gli insegnanti, dunque, dovrebbero essere pronti a cogliere tale sfida anche grazie alla possibilità di formazione permanente offerta loro in primis dalla nostra scuola , in modo da rispondere ai diversi bisogni formativi della classe.

Tale necessità è stata amplificata con l'avvento della DAD e della DID che ha sollecitato la Scuola ad organizzare Formazione interna dei docenti all'uso di Piattaforme e programmi didattici digitali.

https://www.icpraia.edu.it/12-articoli-vari/877-formazione-sofia-42978-ambienti-di-apprendimento-in-situazione-e-a-distanza.html

---

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.

I momenti di formazione e aggiornamento saranno pensati e creati a partire dall'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica; dall'analisi del fabbisogno conoscitivo circa particolari argomenti che si sentono come più cogenti per i docenti e l'Istituto; dall'analisi delle richieste che provengono dagli studenti e dalle studentesse in modo, poi, da riutilizzarli nel loro lavoro di educatori (attraverso le modalità che il docente indica e ritiene più confacente alla classe) quanto appreso durante la formazione ricevuta.

Sul sito istituzionale della nostra scuola, è stata dedicata un'area al Bullismo e Cyberbullismo contenente link e materiali informativi del progetto Generazioni connesse e ulteriori approfondimenti.

https://www.icpraia.edu.it/scuola/pnsd-buone-pratiche/420-generazioni-connesse-2017.html

La scuola si impegna ad aggiornare costantemente l'area di strumenti didattici per tutto il corpo docente da usare con gli studenti e le studentesse, per ciascun grado di scuola.

Si impegna altresì a monitorare le azioni svolte per mezzo di specifici momenti di valutazione.

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.

L'alleanza Scuola-Famiglia nella prevenzione dei rischi connessi ad un uso non consapevole delle TIC è di fondamentale importanza per una efficia delle azioni intraprese.

Ciò in continuità anche con l'art. 5 (comma 2) della legge 29 maggio 2017, n.71 "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo" che prevede l'integrazione, oltre che del regolamento scolastico, anche del "**Patto di Corresponsabilità",** con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari "commisurate alla gravità degli atti compiuti", al fine di meglio regolamentare l'insieme dei provvedimenti sia di natura disciplinare che di natura educativa e di prevenzione al fenomeno.

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.

Il patto di corresponsbilità sarà aggiornato nelle seguenti parti:

- regole sull'uso delle tecnologie digitali da parte dei genitori nelle comunicazioni con la scuola e con i docenti (es. mail, gruppo whatsapp, sito della scuola etc.) e informarli adeguatamente anche riguardo alle regole per gli studenti e le studentesse;
- consigli ai genitori sull'uso delle tecnologie digitali nella comunicazione con i figli e in generale in famiglia.
- sensibilizzare la consultazione della sezione dedicata sul sito www.generazioniconnesse.it

La scuola si impegna a:

- organizzare percorsi di sensibilizzazione e formazione dei genitori su un uso responsabile e costruttivo della Rete in famiglia e a scuola.
- prevedere azioni e strategie per il coinvolgimento delle famiglie in tali percorsi di sensibilizzazione, ad esempio, mediante l'organizzazione di iniziative in cui anche gli studenti e le studentesse siano protagonisti.

Il nostro piano d'azioni

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

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

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

- 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.

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.

La protezione dei dati personali è un diritto fondamentale dell'individuo ai sensi della Carta dei diritti fondamentali dell'Unione europea.

Anche nella nostra scuola vengono trattate giornalmente numerose informazioni sugli studenti e le studentesse, sulle loro famiglie, sui loro problemi sanitari o di disagio sociale, per questo motivo mostriamo sempre massima attenzione all'utilizzo di dati sensibili (quelli più delicati) di un minorenne, o un avviso scolastico con riferimenti indiretti sulle condizioni di salute degli/lle studenti/esse, per evitare di violare anche involontariamente la riservatezza e la dignità di una persona,

La diffusione sempre maggiore di smartphone tra i giovanissimi, l'uso di tablet a scopo didattico, la condivisione online di contenuti didattici, l'uso del registro elettronico, l'eventualità di gruppi whatsapp tra studenti/esse, genitori, docenti o tra insegnanti e studenti/esse, obbliga la scuola ad avere un'attenzione particolare non solo alla privacy in generale, ma anche alla gestione della privacy legata all'uso dei nuovi dispositivi. La velocità con cui si condividono foto o video, può far perdere il controllo di dati personali e mettere a rischio la reputazione e la sicurezza dei soggetti coinvolti.

La scuola, quindi, non ha solo il compito di tutelare la privacy degli/lle studenti/esse e delle loro famiglie, ma anche quello di informare e soprattutto rendere consapevoli gli/le studenti/esse di quanto sia importante tutelare il diritto alla riservatezza di se stessi e degli altri.

Il nostro Istituto Scolastico in conformità al al Regolamento UE 2016/679 deve:

- Redigere e mantenere un registro dei trattamenti dei dati: sia per il titolare che per il responsabile dei trattamenti.
- Valutare i rischi sulla privacy: (definita nel regolamento Data Protection Impact Assessment o PIA) relativamente ad alcune tipologie di trattamento dei dati sensibili. Le istituzioni scolastiche pubbliche e private possono trattare anche dati sensibili, come ad esempio dati relativi alle origini razziali per favorire l'integrazione degli/lle alunni/e, dati relativi alle convinzioni religiose, al fine di garantire la libertà di culto, e dati relativi alla salute per adottare misure di sostegno degli/lle alunni/e, come i dati vaccinali con le Asl.
- Analizzare il processo sulla raccolta/gestione del consenso:
- occorre verificare che la richiesta di consenso sia chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato (art. 7.2), per esempio, all'interno di modulistica o sul proprio sito web istituzionale.
- Prestare attenzione alla formula utilizzata per chiedere il consenso: deve essere comprensibile, semplice e chiara (art. 7.2).

- I soggetti pubblici non devono, di regola, chiedere il consenso per il trattamento dei dati personali, ma devono ad esempio adeguare tutta la modulistica al Regolamento UE 2016/679 e predisporre una lettera di incarico per il trattamento dei dati al personale ATA, ai collaboratori scolastici e ai docenti.
- Adottare idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti:analisi del sito web istituzionale di riferimento con proposte volte a migliorare la sicurezza e la protezione dei dati trattati.
- Proposte in messa in sicurezza della intranet scolastica sulle reti Wi-fi installate.
- Utilizzo di black list per la navigazione (sistemi di filtraggio dei contenuti),
- Uso di un firewall hardware (componente hardware che, utilizzando un certo insieme di regole predefinite, permette di filtrare ed eventualmente bloccare tutto il traffico da e verso una qualsiasi rete di computer, lasciando passare solo tutto ciò che rispetta determinate regole);
- Istituire corsi di formazione destinati ai responsabili, agli incaricati ed eventualmente ai subincaricati del trattamento.

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.

Per questo motivo il nostro Istituto è attento a queste tematiche e si impegna a realizzare e potenziare tutte le attività e procedure per creare ambienti di apprendimento con le caratteristiche indicate, partecipando, infatti, a bandi di implementazione e strumentazione, ad esempio, per le classi virtuali.
Nel particolare, la nostra scuola è dotata di:
- accesso internet in tutte le classi attraverso una rete WI-FI adeguata al numero di studenti e in grado di supportare il traffico dati generato da un numero elevato di utenti (gli alunni possono usufruire della connessione solo tramite pc dell'istituto);
- connessione ad internet tramite collegamento wireless.La Dirigenza e l'Amministrazione hanno una rete separata;
- connessione in tutte le aree della scuola;
- laboratori di informatica con software di controllo gestito dal docente.
Per quanto riguarda l'accesso ad internet, filtri, antivirus e navigazione, il nostro Istituto presenta un proxy server per monitorare il traffico web e per bloccare l'accesso a siti inappropriati a un contesto scolastico.
Occorre, inoltre, sensibilizzare tutta la comunità scolastica sull'opportunità di mantenere aggiornati gli antivirus installati sui dispositivi personali e controllare i dispositivi di archiviazione esterna che vengano collegati al proprio pc.

GSuite for Education

L'Istituto IC PRAIA A MARE ha attivato, inoltre, i servizi della piattaforma G-Suite for Education che Google mette gratuitamente a disposizione delle scuole e delle università. Questa "Suite" è costituita da un insieme di applicazioni (posta elettronica, documenti condivisi (Google drive), calendario, siti web (Sites) e Google Classroom (classi virtuali). Con le GSfE la proprietà dei dati rimane in capo all'utente, con totale protezione e privacy e priva di pubblicità, mentre per gli account privati le possibilità di "intromissione" da parte di Google sono numerose. L'obiettivo di questa iniziativa è ottimizzare, attraverso le tecnologie di rete, l'attività didattica e la circolazione delle

informazioni interne, come comunicazioni, documentazione e didattica (tramite uso di applicazioni specifiche). le attività della "G-Suite for Education" consentono di gestire in modo efficace il flusso informativo all'interno dell'istituto attraverso tre strumenti principali e relative applicazioni:

●Comunicazione: Gmail, Meet, Hangouts, Calendar,gruppi Google+

● Archiviazione: Drive

● Collaborazione: Condivisione di Documenti,fogli, presentazioni, moduli, Sites e di Google Classroom per la gestione di una classe virtuale.

● ad ogni studente è stata assegnata una casella postale composta dal proprio nome, cognome, seguita dal nome di dominio della scuola, esempio: **nome.cognome@icpraia.edu.it**

Gli studenti, già durante la DAD, hanno utilizzato la casella di posta all'interno del dominio @icpraia.edu.it e ad uso esclusivo per le attività della scuola. Anche in quest'anno scolastico, in virtù della DDI, l'Istituto
continuerà ad utilizzare i servizi offerti da GSuite for Education.

Per lavorare bene insieme si sono stabilite ovviamente delle regole di comportamento rese note attraverso la relativa liberatoria. Lo studente, infatti, riceverà la password per accedere ai servizi di Google Suite for Education solo quando lui e un suo genitore/tutore avranno preso atto delle regole di utilizzo, dichiarando così di averle accettate e di essere a conoscenza della normativa locale, nazionale ed europea vigente. È solo in tal modo che lo studente avrà accesso alla piattaforma di Google Suite for Education.

Lo studente si impegna:

 a conservare la password personale e a non consentire l'uso ad altre persone;

a comunicare immediatamente attraverso email a **csic8au004@istruzione.it** l'impossibilità di accedere
al proprio account o il sospetto che altri possano accedervi;

 a non consentire ad altri, a nessun titolo, l'utilizzo della piattaforma Google Suite for Education;

 a non diffondere eventuali informazioni riservate di cui venissero a conoscenza,relative all'attività delle altre persone che utilizzano il servizio;

 ad osservare il regolamento, pena la sospensione da parte dell'Istituto dell'account personale dello studente;

 ad utilizzare i servizi offerti solo ad uso esclusivo per le attività didattiche della scuola.

Lo studente e la sua famiglia si assumono la piena responsabilità di tutti i dati da lui inoltrati,creati e gestiti attraverso la piattaforma Google Suite for Education.

Di conseguenza, lo studente sottoscrive anche le regole di comportamento – la cui infrazione comporterà sanzioni - affinché il servizio possa funzionare nel miglior modo possibile, tenendo presente che cortesia ed educazione, che regolano i rapporti comuni tra le persone,valgono anche in questo contesto.

Di seguito la **Netiquette** indicata nella liberatoria:

1. Poiché il servizio è uno dei mezzi di comunicazione tra Docenti e lo Studente, dovrai accedere alla piattaforma con frequenza quotidiana;

2. se utilizzi un PC non esclusivamente tuo userai sempre il software Google Chrome o Firefox in modalità NAVIGAZIONE IN INCOGNITO;
3. in POSTA e in GRUPPI invierai messaggi brevi che descrivono in modo chiaro di cosa stai parlando; indicherai sempre chiaramente l'oggetto in modo tale che il destinatario possa immediatamente individuare l'argomento della email ricevuta;
4. non inviare mai lettere o comunicazioni a catena che causano un inutile aumento del traffico in rete;
5. non utilizzare la piattaforma in modo da danneggiare,molestare o insultare altre persone;

6. non creare e non trasmettere immagini,dati o materiali offensivi, osceni o indecenti;
7. non creare e non trasmettere materiale offensivo per altre persone o enti;
8. non creare e non trasmettere materiale commerciale o pubblicitario se o espressamente richiesto;
9. quando condividi documenti non interferire, danneggiare o distruggere il lavoro dei tuoi docenti o dei tuoi compagni;
10. non curiosare nei file e non violare la riservatezza degli altri studenti;
11. usa il computer e la piattaforma Google Suite for Education in modo da mostrare considerazione e rispetto per compagni e insegnanti.
L'Istituto, dunque, in relazione alle direttive e alle indicazioni, si impegna alle seguenti azioni per la **cybersecurity**:
- Mantenere separate le reti didattica e segreteria;
- aggiornare periodicamente software e sistema operativo;
- definire la programmazione di backup periodici;
- garantire formazione adeguata allo staff, incluso il corpo docenti;
- testare regolarmente le possibili vulnerabilità;
- preparare piani di azione in risposta ai problemi più seri;
- predisporre la disconnessione automatica dei dispositivi, dopo un certo tempo di inutilizzo;
- impostare il browser per eliminare dei cookies alla chiusura;
- definire una policy sulla password: le password devono essere forti;
- minimizzare i privilegi amministrativi;
- sviluppare il regolamento sull'uso delle tecnologie a scuola (policy di uso accettabile).
Si allegano, inoltre, anche le 'Linee Guida in tema di privacy e sicurezza informatica' approvate dal nostro istituto all'interno del **Regolamento per lo svolgimento delle sedute collegiali in modalità telematica.**

3.3 - Strumenti di comunicazione online

Le tecnologie digitali sono in grado di ridefinire gli ambienti di apprendimento, supportando la comunicazione a scuola e facilitando un approccio sempre più collaborativo. L'uso degli strumenti di comunicazione online a scuola, al fianco di quelli più tradizionali, ha l'obiettivo di rendere lo scambio comunicativo maggiormente interattivo e orizzontale. Tale uso segue obiettivi e regole precise correlati alle caratteristiche, funzionalità e potenzialità delle tecnologie digitali.

Il nostro istituto dispone dei seguenti strumenti di comunicazione:

a) **Sito web della scuola**

La scuola è dotata di sito internet https://www.icpraia.edu.it/

Il sito si configura come un'area pubblica per le informazioni che non comportano la diffusione di dati personali o riservati, in cui sono reperibili le informazioni sulla vita scolastica, iniziative e scadenze ministeriali e avvisi di carattere generale.

L'inserimento dei contenuti è possibile agli addetti del personale di Segreteria, per quanto riguarda i dati di tipo economico-amministrativo; L'Animatore Digitale gestiscono le pagine di Documentazione Didattica dell'Istituto e delle attività che vi si svolgono, nonchè il Calendario delle Attività dei Docenti.

L'AD, che è in possesso delle credenziali per la gestione dei contenuti sul portale, si assume la responsabilità editoriale di garantire che il contenuto inserito sia accurato e appropriato, anche e soprattutto ai fini del rispetto del Codice dell'Amministrazione Digitale (CAD).

b) **Registro elettronico**

Fra gli strumenti di comunicazione interna si annovera il Registro Elettronico, con tutte le sue funzionalità. Le famiglie, così, possono visualizzare molte informazioni utili, interagendo con la scuola, in merito a:

- andamento scolastico;

- risultati scolastici (voti, documenti di valutazione);

-eventi;

- comunicazioni varie.

c) G-Suite for Education (cfr. paragrafo 3.2)

d) Strumenti di comunicazione online per la circolazione di informazioni e comunicazione interne.

In riferimento all'uso degli strumenti di comunicazione online per la circolazione di informazioni e comunicazioni interne, come avviene generalmente fra i docenti mediante ad esempio l'uso di gruppi Whatsapp o Telegram, è importante ricordare quello che si può definire "diritto alla disconnessione". L'art. 22 (Livelli, soggetti, materie di relazioni sindacali per la Sezione Scuola) del CCNL 2016/2018, infatti, fa riferimento ai criteri generali per l'utilizzo di strumentazioni tecnologiche di lavoro in orario diverso da quello di servizio, al fine di una maggiore conciliazione fra vita lavorativa e vita familiare.

Lo stato emergenziale vissuto nell'a.s. 2019/2020 ha favorito la comunicazione informale fra colleghi e docenti, nonché eccezionalmente anche un primo raggiungimento degli allievi e delle famiglie, allo scopo di attivare in tempi brevi la didattica a distanza.
È importante sottolineare, comunque, che non esiste una vera e propria regolamentazione per la circolazione di informazioni e di comunicazione interne tramite gli strumenti online e, per tale ragione è fondamentale, a partire dal buon senso e da una riflessione sulle peculiarità del mezzo, predisporre comunque delle regole condivise sull'uso delle stesse, come quelle indicate di seguito:

- 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;
- non condividere file multimediali troppo pesanti;
- evitare il più possibile di condividere foto di studenti in chat;
- 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.

Si ricorda, inoltre, quando si usano invece chat formali, create ad esempio dal Dirigente scolastico per veicolare messaggi, informazioni e aggiornamenti relativi all'attività scolastica, la regolamentazione è prevista dalla contrattazione di Istituto.

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.

PER LA COMPONENTE STUDENTESCA

 I telefoni cellulari, i tablet e le relative fotocamere e registratori vocali non verranno utilizzati durante le lezioni scolastiche se non all'interno di attività didattiche espressamente programmate dal corpo docente.

 L'insegnante della prima ora ricorda agli alunni di spegnere i cellulari (si rimanda al Regolamento d'Istituto che disciplina le diverse sanzioni per l'uso improprio del dispositivo mobile).

 Alunni con disturbi specifici di apprendimento, previa consultazione con il Consiglio di Classe, concorderanno le modalità di impiego di strumenti compensativi quali tablet e computer portatili e le modalità di custodia degli stessi.

 Giochi e console, tra cui la Sony Playstation, Microsoft Xbox e similari, che possono avere accesso a Internet non filtrato, non sono consentiti nemmeno se custoditi come previsto per gli altri dispositivi. Saranno requisiti dal docente che ravvisa l'infrazione, depositati in dirigenza e consegnati al genitore/tutore convocato, che sarà contestualmente informato dell'eventuale sanzione disciplinare comminata al trasgressore.

 Nel caso in cui debbano comunicare con la famiglia durante l'orario scolastico, alunne e alunni possono usare gratuitamente la linea fissa della scuola rivolgendosi a un operatore; allo stesso modo le famiglie devono chiamare il centralino della scuola se hanno assoluta necessità di parlare con i propri figli. Si raccomanda di ridurre tali comunicazioni a casi di inderogabile necessità e urgenza.

 L'invio di materiali abusivi, offensivi o inappropriati è vietato, anche se avviene all'interno di cerchie o gruppi di discussione privati.

PER IL PERSONALE DOCENTE/ATA

 Il personale preferirà, quando ciò è possibile, l'impiego della strumentazione personale rispetto a quella fornita dalla scuola (portatili, pc fissi, …).
 le infrastrutture e gli apparati della scuola non vanno utilizzati per scopi personali.
 Telefoni cellulari, tablet, fotocamere e altri strumenti di registrazione audio/video non devono essere impiegati durante le lezioni scolastiche se non all'interno di attività didattiche espressamente programmate.
 La password di accesso alla rete va custodita con cura e per nessuna ragione deve essere divulgata a chi non ha titolo per utilizzarla (studenti, genitori,

operatori esterni).

 Qualora si utilizzino a scuola dispositivi di archiviazione esterna di proprietà personale (chiavette usb, dischi fissi portatili) è bene controllare preventivamente che essi siano esenti da virus per evitare di danneggiare le attrezzature comuni.

Durante l'attività didattica è opportuno che ogni insegnante:

 Dia chiare indicazioni sul corretto utilizzo della rete (Internet, piattaforma studenti, ecc.), condividendo con gli studenti la netiquette e indicandone le regole;

 si assuma la responsabilità di segnalare prontamente eventuali malfunzionamenti o danneggiamenti in Segreteria, all'AD o al tecnico informatico;

 non salvi sulla memoria locale della postazione di classe file contenenti dati personali e/o sensibili e proponga agli alunni attività di ricerca di informazioni in rete fornendo opportunamente loro indirizzi dei siti e/o parole chiave per la ricerca cui fare riferimento.

UTILIZZO DEL LABORATORIO DI INFORMATICA E DELLE POSTAZIONI DI LAVORO

La scuola è già dotata di un regolamento di fruizione e di utilizzo del laboratorio di informatica, tuttavia è utile,

in questa Policy, ricordare le disposizioni generali sull'uso dei laboratori:

1. Le apparecchiature presenti nella scuola sono patrimonio comune, quindi, vanno utilizzate con il massimo rispetto.
2. I laboratori informatici e le postazioni informatiche dell'istituto possono essere utilizzati esclusivamente per attività di insegnamento, funzionali all'insegnamento e di formazione del personale docente e non docente.
3. Quando un insegnante, da solo o in classe, usufruisce del laboratorio deve registrare il proprio nome e l'eventuale classe nell'apposito registro delle presenze di laboratorio, indicando il numero della postazione utilizzata per sè e per ogni alunno. Questo allo scopo di poter risalire alle cause di eventuali inconvenienti o danneggiamenti e per comprovare l'effettivo utilizzo dell'aula.
4. L'ingresso degli allievi nei laboratori è consentito solo in presenza dell'insegnante.
5. Il docente accompagnatore è responsabile del corretto uso didattico di hardware e software.
6. Nei laboratori è vietato utilizzare CD personali, USB o altri dispositivi se non dopo opportuno controllo con sistema di antivirus aggiornato.
7. All'uscita dal laboratorio sarà cura di chi lo ha utilizzato lasciare il locale in ordine e le macchine spente correttamente, avvisando il Collaboratore Scolastico se restano accese in aggiornamento.
8. In caso di malfunzionamento o guasto dei computer bisogna darne tempestiva segnalazione al responsabile del laboratorio.
9. L'accesso a Internet è consentito al personale docente e non docente solo ad esclusivo uso didattico e/o di formazione e alle classi accompagnate e sotto la responsabilità di un insegnante.

Il Responsabile di laboratorio che verifichi un uso del laboratorio contrario a disposizioni di legge o del regolamento interno deve darne comunicazione per iscritto

al Dirigente Scolastico.

Il nostro piano d'azioni

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

Scegliere almeno 1 di queste azioni:

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte deglistudenti e delle studentesse
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte dei docenti
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte delpersonale Tecnico Amministrativo e dagli ATA
- Organizzare uno o più eventi o attività volti a consultare i docenti dell'Istituto perredigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola
- Organizzare incontri per la consultazione degli studenti/studentesse suindicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola
- Organizzare incontri per la consultazione dei genitori su indicazioni/regolamentisull'uso dei dispositivi digitali personali a scuola
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare i genitori dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

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

Scegliere almeno 1 di queste azioni:

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli studenti e delle studentesse
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte dei docenti
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte delpersonale Tecnico Amministrativo e dagli ATA
- Organizzare uno o più eventi o attività volti a consultare i docenti dell'Istituto perredigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali.
- Organizzare incontri per la consultazione degli studenti/studentesse suindicazioni/regolamenti sull'uso dei dispositivi digitali personali
- Organizzare incontri per la consultazione dei genitori su indicazioni/regolamentisull'uso dei dispositivi digitali personali
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare i genitori dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

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

4.1 - Sensibilizzazione e Prevenzione

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

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

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

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

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

È importante che i minori abbiano gli strumenti idonei per riconoscere possibili situazioni di rischio e segnalarle ad un adulto di riferimento.

Gli strumenti che **l'IC Praia a Mare** adotta per poter ridurre l'incidenza di situazioni di rischio si configurano come

interventi di **sensibilizzazione e prevenzione.**

Sensibilizzazione

A partire dalle classi quinte della scuola primaria sino all'intero ciclo della secondaria, si punta a informare ma soprattutto ad educare alla consapevolezza e alla riflessione sulle seguenti tematiche:

- Uso o abuso di internet
- Quanto sono dipendente dallo smartphone, che uso ne faccio, per quante ore nell'arco della giornata, riesco a darmi delle regole?
- Come la rete ha modificato il mio modo di comunicare e di pormi in relazione con l'altro; i gruppi whatsapp, la messaggistica, sostituiscono il linguaggio verbale e non verbale?
- Quanto sono consapevole dei pericoli della rete, cosa penso di sapere, come penso di evitarli?
- Favorire la diffusione di informazioni e servizi disponibili all'utilità collettiva (promuovere la
  conoscenza dell'ePolicy nella comunità scolastica).

In sintesi, è opportuno tenere in considerazione i seguenti aspetti:

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

Prevenzione

Prevenzione Universale Un programma di questo tipo parte dal presupposto che tutti gli studenti siano potenzialmente a rischio.

Si tratta quindi di interventi che mirano a:

- Fermare l'evoluzione del problema e contrastarne la manifestazione
- Ridurre l'impatto sociale e personale di un comèportamento problematico.
- Rafforzare le competenze, le attitudini e i comportamenti che promuovono il benessere.

La prevenzione Universale si rivolge all'intera popolazione scolastica quindi alunni, docenti, non docenti, genitori.

Si tratta quindi di interventi che possono produrre cambiamenti in
grandi popolazioni (ad es. si pensi ad un programma dedicato alle competenze emotive, oppure alla cittadinanza digitale).

Prevenzione Selettiva

La prevenzione selettiva viene rivolta 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.

Prevenzione Indicata

Viene messo in campo un 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, supportati dallo psicologo della Scuola.

La responsabilità dell'azione preventiva ed educativa chiama in campo diverse agenzie educative oltre alla scuola, come la famiglia, ma non solo (istituzioni, associazioni, società civile, etc.), ciascuna con un proprio compito nei confronti di bambini e bambine e di adolescenti.

Tali agenzie sono chiamate a collaborare ad un progetto comune, nell'ambito di funzioni educative condivise. La necessità di questa collaborazione nasce, più o meno consapevolmente, dal riconoscimento sia da parte dei genitori che da parte degli insegnanti della rispettiva difficoltà a svolgere da soli la propria funzione formativa ed educativa.

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).

Come previsto dalla legge, l'I.C. Praia a Mare ha:

- Nominato un **referente** che si occupa della prevenzione e del contrasto del bullismo e cyberbullismo
- Aggiornato il Regolamento di Istituto antibullismo-cyberbullismo
- Stipulato un Protocollo di Emegenza

https://www.icpraia.edu.it/attachments/article/420/Bullismo%20e%20cyberbullismo%20allegati.zip

- Istituito un Team di docenti adeguatamente formati sul tema per la gestione casi .
- Realizzato un Sistema di Tutela in collaborazione con l'Associazione Edi attraverso il progetto SCATTI.
- Promosso un ruolo attivo degli studenti per attività di peer education.

Il regolamento include una parte dedicata all'uso di Internet in cui 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 removibili personali senza autorizzazione
■ tenere spento lo smartphone al di fuori delle attività didattiche che ne prevedano l'utilizzo

■ durante le attività che prevedono lo smartphone, utilizzarlo esclusivamente per svolgere le attività didattiche previste.

Nel Protocollo di Emergenza è previsto una scheda di segnalazione di eventuali atti di bullismo e/o cyberbullismo.
- Individuato le procedure di intervento in caso di segnalazione.
- Pubblicato sul sito della scuola, a conoscenza delle famiglie e di tutti gli alunni, tale regolamento, incluso la scheda di segnalazione che può essere compilata e inviata via mail o consegnata in formato cartaceo al Responsabile di plesso.

Sempre sul sito, nella sezione dedicata, è altresì pubblicato una guida per i genitori, con riferimenti di siti, servizi, numeri telefonici per un supporto psicologico e legale in caso di problematiche legate al bullismo e/o cyberbullismo. In questa guida sono indicati i segnali generali che può manifestare la vittima.

La normativa in materia

Il Parlamento italiano ha approvato il 18 maggio 2017 la Legge 71/2017, Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del Cyberbullismo, una legge a tutela dei
minori per la prevenzione e il contrasto al cyberbullismo che prevede misure prevalentemente a carattere educativo/rieducativo.

La legge pone al centro il ruolo dell'istituzione scolastica nella prevenzione e nella gestione del fenomeno e ogni Istituto scolastico dovrà provvedere ad individuare fra i docenti un referente con il compito di coordinare le iniziative di prevenzione e di contrasto del cyberbullismo. Questi aspetti vengono chiariti nel dettaglio dalle Linee di orientamento per la prevenzione e il contrasto del cyberbullismo

http://www.miur.gov.it/documents/20182/0/Linee+Guida+Bullismo+-+2017.pdf/4df7c320-e98f-4417-9c31-9100fd63e2be?version=1.0

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.

Più precisamente: *Chi compie atti di bullismo e cyberbullismo può anche essere responsabile di reati penali e danni civili.*

I ragazzi e le ragazze che fanno azioni di bullismo possono commettere reati. Secondo il codice penale italiano i comportamenti penalmente rilevanti in questi casi sono:

- ***percosse (art. 581),***
- ***lesione personale (art. 582),***
- ***ingiuria (art. 594),***
- ***diffamazione (art. 595),***
- ***violenza privata (art. 610),***

- ***minaccia (art. 612),***
- ***danneggiamento (art. 635).***

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 il nostro ordinamento l'imputabilità penale (ossia la responsabilità personale per i reati commessi) scatta al quattordicesimo anno. La legge sancisce che "nessuno può essere punito per un fatto preveduto dalla legge come reato, se al momento in cui l'ha commesso, non era imputabile". Cosa si intende per "imputabilità"? Vuol dire avere la cosiddetta "capacità d'intendere e volere".

Per poter avviare un procedimento penale nei confronti di un minore, quindi 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)

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 (così come previsto anche dalla normativa vigente).

Responsabilità dei genitori

Se il minore non ha compiuto i 14 anni, non risponde penalmente per l'evento, ma i genitori saranno tenuti al risarcimento del danno, per presunta "culpa in educando", così come previsto dal codice civile per i fatti commessi dal figlio. Non c'è responsabilità penale dei genitori, perché la responsabilità penale è personale.
Se i genitori riescono a fornire la prova di aver fatto di tutto per impedire il fatto,

possono essere esonerati dall'obbligo di risarcire il danno causato dal figlio. Ma questo tipo di prova è molto
difficile da produrre, perché significa poter dare evidenza certa:
di aver educato e istruito adeguatamente il figlio (valutazione che viene dal giudice commisurata alle circostanze, ovvero tra l'altro alle condizioni economiche della famiglia e all'ambiente sociale a cui appartiene),di aver vigilato attentamente e costantemente sulla sua condotta, di non aver in alcun modo potuto impedire il fatto, stante l'imprevedibilità e repentinità, inconcreto, dell'azione dannosa.

Responsabilità degli insegnanti

In quali momenti l'insegnante è responsabile?

Va considerato tutto il tempo dell'affidamento dell'alunno alla scuola. Quindi, non soltanto le ore delle attività didattiche, ma anche tutti gli altri momenti della vita scolastica, compresa la ricreazione, la pausa pranzo, la palestra, le uscite e i viaggi di istruzione etc.

Gli insegnanti potranno essere chiamati a rispondere personalmente solo in caso di azione di rivalsa per dolo o colpa grave, da parte dell'amministrazione. L'insegnante ha un dovere di vigilanza e di conseguenza viene addebitata, in caso di comportamento illecito del minore affidato, una colpa presunta, cioè una "culpa in vigilando", come inadempimento dell'obbligo di sorveglianza sugli allievi. Di questa colpa/responsabilità si può essere liberati dimostrando di non aver potuto impedire il fatto. Si tiene conto in questi casi dell'età e del grado di maturità dei ragazzi, della concreta situazione ambientale, etc.

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.

Come intervenire?

Lo sviluppo delle competenze digitali e l'educazione ad un uso etico e consapevole delle tecnologie assumono quindi un ruolo centrale anche per la promozione della consapevolezza di queste dinamiche in rete.

La nostra scuola in tal senso si propone di fornire ai più giovani gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di hate speech, e promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network.

La realizzazione di un UDA trasversale "Gentil-net" ha avuto lo scopo di fornire a tutti gli alunni del nostro Istituto, dall'infanzia alla Secondaria di I grado, la consapevolezza dell'unicità dell'individuo e quindi del rispetto della propria identità.

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?

Negli ultimi anni si è registrato un aumento esponenziale del fenomeno nei ragazzi dai 11 ai 17 anni che usano lo smartphon oltre 3 ore al giorno per giocare, messaggiare navigare in internet, seguire i profili social personali e di altri.

I sintomi della dipendenza da Internet

- il bisogno di trascorrere in rete un tempo sempre maggiore e di connettersi sempre più spesso, per ottenere soddisfazione
- la marcata riduzione dell'interesse per ogni altra attività che non riguardi l'uso di Internet
- se l'abuso viene ridotto o interrotto, la persona sviluppa agitazione, sintomi depressivi e ansiosi, pensieri ossessivi o sogni su quello che sta accadendo in rete
- l'incapacità di interrompere o tenere sotto controllo l'utilizzo di Internet
- continuare ad usare il web nonostante la consapevolezza di aver sviluppato dei problemi di ordine sociale, psicologico e fisico (difficoltà del sonno, problemi familiari),

Da un punto di vista cognitivo – comportamentale, negli adolescenti che sviluppano una **dipendenza da Internet**, sono osservabili i seguenti aspetti:

- pensieri disfunzionali su se stessi e sugli altri
- sentimenti soggettivi di inadeguatezza, insicurezza, bassa autostima e problemi relazionali
- disturbi dell'umore, d'ansia e del controllo degli impulsi.

Il nostro Istituto si impegna a promuove azioni di prevenzione attraverso percorsi sul benessere digitale attraverso:

- Conferenze di varia natura rivolto a genitori, insegnanti e studenti
- Formazione ai docenti
- Attivazione di supporto psicologico
- Azioni di sensibilizzazione sull'importanza di trarre vantaggi dalla rete evidenziando nel contempo i pericoli legati alla dipendenza dalla stessa.

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.

Con queste parole si intende generalmente lo scambio messaggi, audio, immagini o video - specialmente attraverso smartphone o chat di social network - a sfondo

sessuale o sessualmente espliciti, comprese immagini di nudi o seminudi. Questo fenomeno si è molto diffuso negli ultimi anni, anche tra i minori.

I contenuti sessualmente espliciti, quindi, possono diventare materiale di ricatto assumendo la forma di "revenge porn" letteralmente "vendetta porno" fenomeno quest'ultimo che consiste nella diffusione illecita di immagini o di video contenenti riferimenti sessuali diretti al fine di ricattare l'altra parte (la Legge 19 luglio 2019 n. 69, all'articolo 10 ha introdotto in Italia il reato di revenge porn, con la denominazione di **diffusione illecita di immagini o di video sessualmente espliciti**.

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.

Attraverso un'attività didattica mirata, utilizzando i materiali e video forniti anche da Generazioni Connesse, si può intervenire e prevenire questo fenomeno.

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.

Avere un profilo sui social network significa accedere ad un bacino molto ampio di conoscenze virtuali che non si conoscono direttamente nella vita reale. Contare tanti amici online o molti follower è sinonimo di popolarità e per questo gli adolescenti aggiungono spesso alla propria cerchia in Rete numerosi "amici di amici", senza essere pienamente consapevoli del fatto che in questo modo stanno dando accesso a una grande quantità di informazioni private: luoghi che frequentano, foto e molto altro. Questo li espone potenzialmente a rischi importanti, perché queste informazioni possono essere utilizzate dagli sconosciuti in modo inaspettato e con ripercussioni negative nella vita reale.

L'adescamento, quindi, non avviene apparentemente con una dinamica violenta, ma il "**prendersi cura**" del minore rappresenta la conditio per carpirne la fiducia ed instaurare una relazione a sfondo erotico. Può capitare che l'adescatore si presenti al minore sotto falsa identità, fingendo quindi di essere un'altra persona così da attirare maggiormente l'attenzione del minore (ad esempio, potrebbe fingersi un talent scout del mondo dello spettacolo alla ricerca di volti nuovi).

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).

Come intervenire?

Se si sospetta o si ha la certezza di un caso di adescamento online è importante, innanzitutto, che l'adulto di riferimento non si sostituisca al minore nel rispondere, ad esempio, all'adescatore. È importante che il computer o altri dispositivi elettronici del minore vittima non vengano usati per non compromettere eventuali prove.

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

I minori vittime di adescamento riferiscono, generalmente, di sentirsi traditi, ma anche di provare un senso di colpa per essere caduti in trappola ed essersi fidati di uno sconosciuto.

Nei casi più estremi in cui l'adescamento porta ad un incontro fisico e ad un abuso sessuale un sostegno psicologico esperto per il minore è da considerarsi prioritario e urgente.

4.7 - Pedopornografia

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

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

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

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

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

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

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

La pedopornografia esiste da prima dell'avvento di Internet. Tuttavia, la diffusione della Rete, l'evoluzione e la moltiplicazione dei "luoghi" virtuali, il cambiamento costante delle stesse tecnologie digitali, ha radicalmente cambiato il modo in cui il materiale pedopornografico viene prodotto e diffuso, contribuendo ad un aumento della sua disponibilità e dei canali di diffusione. La diffusione della banda larga, ad esempio, consente di caricare e scaricare velocemente video e foto anche di grandi dimensioni, così come la diffusione delle videocamere e dei cellulari con videocamera incorporata, consente la produzione "in house" di materiale video, riproducibile facilmente online.

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, e inoltre prevedere:

- Percorsi di Educazione Civica, Affettiva e Sessuale
- Sensibilizzazione all'uso corretto e consapevole di Ineternet e del cellullare.

Il nostro piano d'azioni

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

Scegliere almeno 1 di queste azioni:

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

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

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

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

☐ Promuovere incontri e laboratori per studenti e studentesse dedicati all'

Educazione Civica Digitale.

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

☐ Organizzare uno o più eventi e/o dibattiti in momenti extra-scolastici, sui temi della diversità e sull'inclusione rivolti a genitori, studenti/studentesse e personale della scuola.

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

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

Scegliere almeno 1 di queste azioni:

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

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

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

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

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

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

☐ Organizzare uno o più eventi e/o dibattiti in momenti extra-scolastici, sui temi della diversità e sull'inclusione rivolti a genitori, studenti/studentesse e

personale della scuola.

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

Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

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

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

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

Nelle procedure:

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

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

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

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

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

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

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

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

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

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

Vi suggeriamo, inoltre, i seguenti servizi:

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

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

segnalare la presenza di materiale pedopornografico online.

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.

Nel nostro Istituto è stato definito un protocollo d'azione con le linee operative per affrontare le emergenze legate ad atti di bullismo e cyberbullismo e di vittimizzazione che arrivano all'attenzione della scuola.

https://www.icpraia.edu.it/scuola/pnsd-buone-pratiche/420-generazioni-connesse-2017.html

Le azioni svolte dal team consistono nella presa in carico della segnalazione di un caso e, successivamente, nella conduzione della valutazione, quest'ultima volta a capire effettivamente se la segnalazione acquisita possa rispondere a criteri di bullismo e vittimizzazione piuttosto che a un conflitto tra pari di natura occasionale. Dopo la valutazione, il team sarà in grado di comprendere la gravità della situazione e di poter scegliere la tipologia più adatta di intervento per gestire il caso. L'ultima fase è quella del monitoraggio, in cui si verificherà se gli interventi messi in atto siano stati funzionali ed efficaci per la risoluzione dei casi, altrimenti sarà necessario ricominciare il processo o ridefinire l'intervento in atto.

Strumenti di segnalazione messi a disposizione degli alunni, dei docenti, dei genitori e del personale ATA:

- Indirizzo email al quale inviare la segnalazione
- Modelli reperibili nell'apposita area denominata "Fermiamo il bullo" o negli spazi predisposti della scuola.
- Scatola/box per la raccolta di segnalazioni in uno spazio della scuola facilmente accessibile e riservato.
- Sportello di ascolto con la figura dello psicologo.
- Docente referente e team delle emergenze per le segnalazioni

La segnalazione potrà avvenire secondo le seguenti modalità:

Gli alunni potranno segnalare il caso attraverso il modulo da compilare obbligatoriamente con nome cognome e che verrà inserito nella scatola/box presente in ogni plesso del nostro Istituto;

I genitori potranno effettuare la segnalazione inviando il modello al responsabile di plesso o a uno dei componenti del team dell'emergenza.
I docenti e il personale Ata potranno inviare o consegnare il modello a mano al responsabile di plesso o a uno dei componenti del team dell'emergenza.

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.

Nella gestione dei casi, qualora la gravità e la sistematicità della situazione richieda inyterventi che esulano dalle competenze della scuola, è necessario rivolgerisi ad altre figure, enti, istituzioni e servizi presenti sul territorio.

Vengono indicati gli attori sul territorio a cui è possibile rivolgersi:

GARANTE REGIONALE PER L'INFANZIA E L'ADOLESCENZA

Segnala all'autorità giudiziaria i servizi sociali e competenti; accoglie le segnalazioni di presunti abusi; fornisce informazioni sulle modalità di tutela e di esercizio di questi diritti; segnala alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.

http://www.garanteinfanzia.consrc.it/index.php

CORECOM

Svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale. Tra le varie attività, particolare attenzione è riservata alla tutela dei minori

http://corecom.consrc.it/hp2/default.asp

UFFICO SCOLASTICO REGIONALE PER LA CALABRIA

Tra le varie funzioni, supporta la scuola in attività di prevenzione. Può affiancare le scuole nei casi di segnalazione di comportamenti a rischio correlati all'uso di internet.

https://www.istruzione.calabria.it/

TRIBUNALE PER I MINORENNI DI CATANZARO

Tra le varie attività si occupa di tutti i procedimenti che riguardano reati, misure rieducative, tutela ed assistenza.

http://www.tribunaleminoricatanzaro.it/

POLIZIA POSTALE E DELLE COMUNICAZIONI

Si occupa di accogliere tutte le segnalazioni o denunce relative a comportamenti a rischio nell'utilizzo di internet e che si configurano come reati.

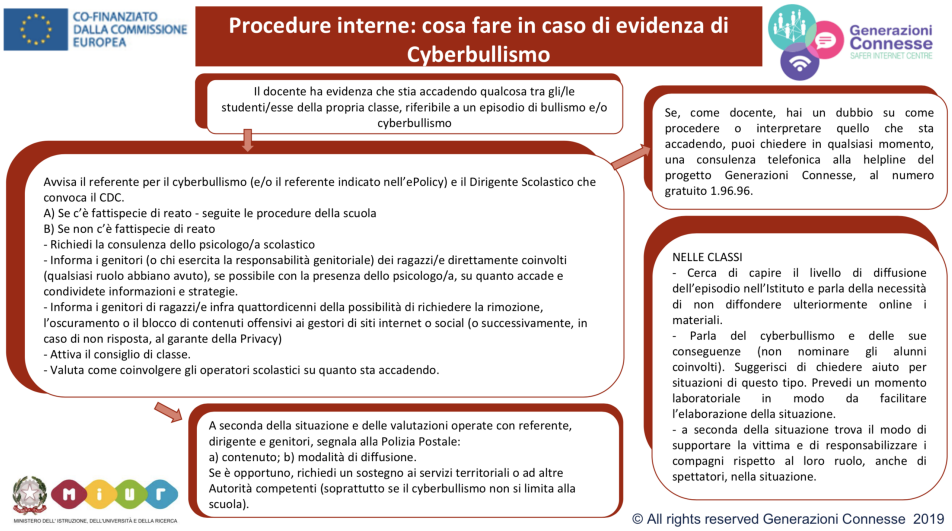
https://www.commissariatodips.it/

AZIENDE SANITARIE LOCALI

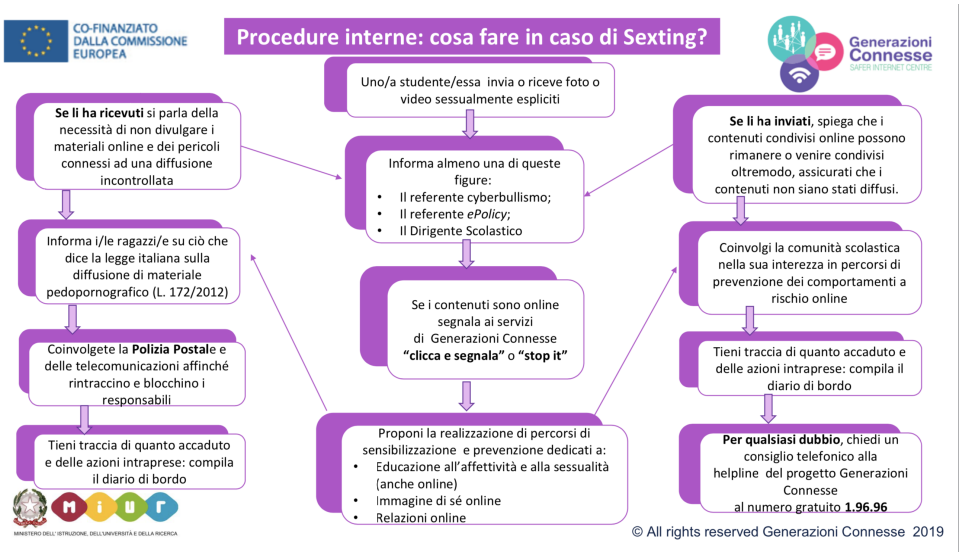
Per avere un sostegno psicologico, psichiatrico o neuropsichiatrico sulle problematiche psicologiche, anche associate all'uso di Internet.

5.4. - Allegati con le procedure

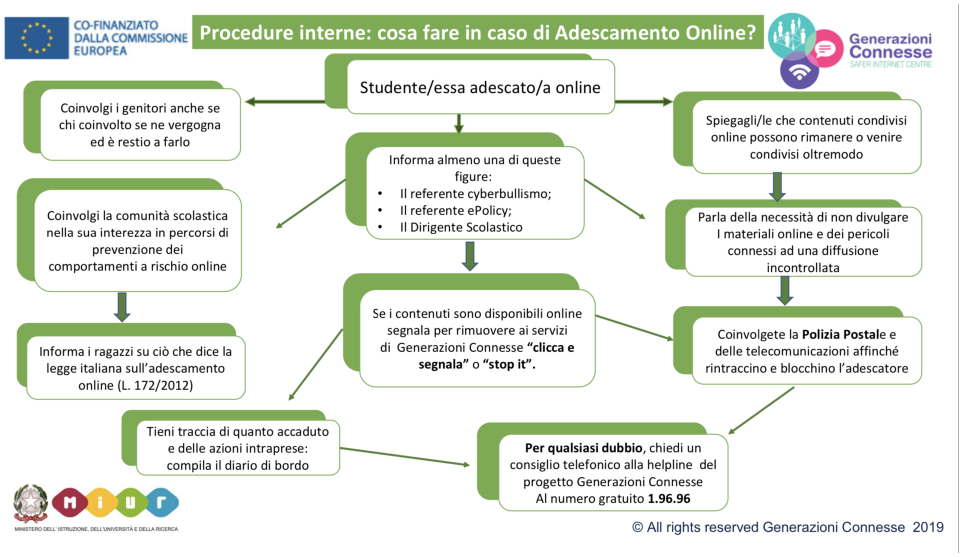
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



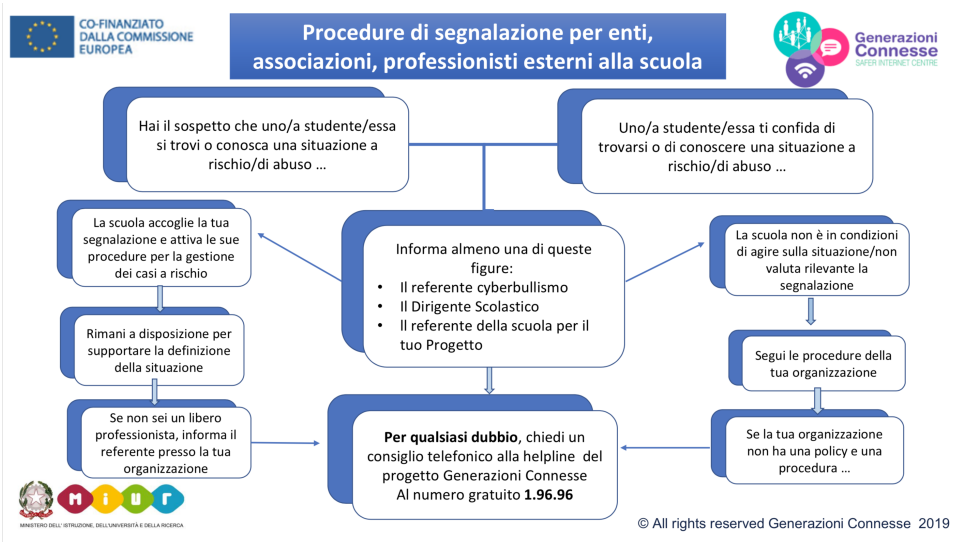
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



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



Altri allegati

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

Il nostro piano d'azioni

- l'IC Praia a Mare si impegna ad aggiornare annualmente il docomento e-policy
- Diffondere informazioni utili alla gestione dei casi ai genitori alunni e personale scolastico.
- Aggiornare la sezione del sito istituzionale "Fermiamo il bullo".
- Garantire un supporto specialistico interno a sostegno di alunni e genitori.