Documento di ePolicy

CLEE02500P

"SAN CATALDO II"

VIA SANTA MARIA MAZZARELLO SNC - 93017 - SAN CATALDO - CALTANISSETTA (CL)

ROSA AMBRA

Capitolo 1 - Introduzione al documento di ePolicy

1.1 - Scopo dell'ePolicy

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

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

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

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

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

Argomenti del Documento

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

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

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

Perché è importante dotarsi di una E-policy?

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

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

La nostra istituzione scolastica ha elaborato questo documento con lo scopo di informare l'utenza per un uso corretto e responsabile delle apparecchiature informatiche collegate alla rete in

dotazione alla scuola, e per gestire, prevenire situazioni problematiche. In particolare il nostro intento è quello di promuovere l'uso adeguato e critico da parte degli alunni delle tecnologie digitali e di internet, di far acquisire loro, non solo competenze "tecniche," ma anche corrette norme comportamentali. Gli utenti, adulti e minori, devono acquisire consapevolezza dei rischi a cui si espongono quando navigano in rete. Per questo motivo, gli insegnanti devono guidare gli studenti nelle attività online a scuola e indicare loro le regole di condotta per l'utilizzo sicuro di internet anche a casa. La nostra Scuola, negli ultimi anni, ha incrementato molto l'uso delle tecnologie informatiche nella didattica e nell'organizzazione generale della scuola, non solo per svolgere esperienze formative, ma anche per condurre in modo più efficiente le funzioni amministrative. Grazie all'implementazione del sito, al registro elettronico e all'utilizzo della piattaforma web Argo, a cui possono accedere Dirigente, docenti, genitori, alunni e personale amministrativo, è diventato più semplice gestire il sistema-scuola e aprire la scuola all'utenza con una comunicazione più tempestiva, chiara e trasparente. Allo stesso tempo, l'uso di piattaforme web ha esposto gli utenti e in particolare i minori e i soggetti con limitate competenze informatiche a nuovi rischi. Per questo la nostra scuola ha deciso di partecipare al progetto "Generazioni Connesse" ed elaborare l'E-Policy per:

- diffondere la conoscenza e comprensione da parte di tutto il personale scolastico delle procedure, monitoraggio e gestione di casi di abuso o di altre problematiche associate all'utilizzo di Internet e delle tecnologie digitali;
- disciplinare l'utilizzo delle TIC all'interno della scuola stessa (dotazione di filtri) e prevedere misure per prevenire diverse tipologie di rischio;
- promuovere la competenza digitale negli alunni e la cultura del rispetto di regole comuni nell'uso dei servizi telematici e lo sviluppo di regole di comportamento (Netiquette) riferite all'utilizzo dei nuovi media.

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.

Nell'ambito di questa E-Policy sono individuati i seguenti ruoli e le principali responsabilità correlate:

Il Dirigente scolastico ha il compito di:

- garantire la sicurezza (tra cui la sicurezza on-line) dei membri della comunità scolastica;
- garantire a tutti gli insegnanti di ricevere una formazione adeguata per svolgere efficacemente l'insegnamento volto a promuovere una cultura dell'inclusione, del rispetto dell'altro/a e delle differenze;
- 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.

L'Animatore digitale

Il ruolo dell'Animatore digitale include i seguenti compiti:

- stimolare la formazione interna all'istituzione sui temi del PNSD (Piano Nazionale 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;
- individuare soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola;
- assicurare che gli utenti possano accedere alla rete della scuola tramite password applicate, regolarmente cambiate e curare lo sviluppo del sito web della scuola;
- coinvolgere la comunità scolastica (alunni, genitori e altri attori del territorio) nella partecipazione ad attività e progetti attinenti il PNSD;
- 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, affinché vengano adottate le procedure previste dalle norme.

Il Referente d'Istituto per il bullismo ed il cyberbullismo:

Ha il compito di coordinare le iniziative di prevenzione e di contrasto del Cyberbullismo, messe in atto dalla scuola, anche avvalendosi della collaborazione delle Forze di Polizia nonché delle associazioni e dei centri di aggregazione giovanile presenti sul territorio (Legge n. 71 del 2017). Inoltre, ha il compito di supportare il Dirigente Scolastico nella revisione e stesura di Regolamenti, atti e documenti (PTOF, PdM, RAV, e-Policy d'Istituto); segnala tempestivamente situazioni di rischio online o casi di bullismo o cyberbullismo.

I Docenti

Il ruolo del personale docente prevede 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, rispettandone il regolamento;
- garantire che gli alunni rispettino le regole per prevenire e contrastare l'utilizzo scorretto e pericoloso delle TIC e di internet;
- 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;
- garantire che le comunicazioni digitali dei docenti con alunni e genitori siano svolte nel rispetto del codice di comportamento professionale ed effettuate con sistemi scolastici

ufficiali;
- assicurare la riservatezza dei dati personali trattati ai sensi della normativa vigente;
- 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, affinché vengano applicate le procedure previste dalle norme.

Il Personale Amministrativo, Tecnico e Ausiliario (ATA)

ll personale Amministrativo, Tecnico e Ausiliario (ATA) svolge funzioni di tipo amministrativo, contabile, gestionale e di sorveglianza, in collaborazione con il dirigente scolastico e con il personale docente. Essi si occupano, ciascuno per la propria funzione, del funzionamento dell'Istituto scolastico attraverso l'uso del digitale e cui compiti sono:

- assicurare, nei limiti delle risorse finanziarie disponibili, gli interventi di manutenzione necessari per garantire che l'infrastruttura tecnica della scuola sia funzionante e controllando al contempo che le norme di sicurezza vengano rispettate.
- registrare i disservizi e le problematiche relative alla rete e all'uso del digitale segnalate dai docenti e provvedere, ove possibile, all'intervento tecnico;
- garantire il funzionamento dei diversi canali di comunicazione della scuola (circolari, sito web, ecc.) all'interno della stessa e fra la scuola e le famiglie degli alunni.

Il personale ATA viene coinvolto nella formazione sul tema del Bullismo, Cyberbullismo e Sicurezza in rete, nella segnalazione dei comportamenti non adeguati e atti di bullismo, nel verificare e valutare le informazioni per riferirli al referente di Istituto e al Dirigente Scolastico.

Gli Alunni

Gli alunni hanno il compito di:

- utilizzare la rete Internet in modo responsabile, consapevole e sicuro secondo quanto richiesto dai docenti;
- comprendere l'importanza di adottare buone pratiche di sicurezza on-line per non correre rischi;
- tutelare i propri compagni e rispettarli;
- partecipare attivamente a progetti ed attività che riguardano l'uso positivo delle TIC e della Rete e farsi promotori di quanto appreso anche attraverso possibili percorsi di peer education;
- 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 di rispettare i diritti d'autore;
- adottare condotte rispettose degli altri anche quando si comunica in rete (Netiquette)
- esprimere domande o difficoltà o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o di internet ai docenti e ai genitori.

I Genitori

I genitori devono:

- essere partecipi e attivi nelle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete nonché sull'uso responsabile dei device personali;
- relazionarsi in modo costruttivo con i docenti sulle linee educative che riguardano le TIC e la Rete e comunicare con loro circa i problemi rilevati quando i/le propri/e figli/e non usano responsabilmente le tecnologie digitali o Internet;
- sostenere la linea di condotta della scuola adottata nei confronti dell'utilizzo delle tecnologie dell'Informazione e delle Comunicazioni nella didattica;
- concordare con i docenti linee di intervento coerenti e di carattere educativo in relazione ai problemi 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;
- accettare e condividere l'ePolicy dell'Istituto.

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).

Tutte le persone esterne che erogano attività educative nel nostro Istituto devono:

- mantenere sempre un elevato profilo personale e professionale, eliminando atteggiamenti inappropriati, ascoltare le opinioni ed i desideri dei minori, soprattutto se preoccupati o

allertati per qualcosa;
- conformarsi alla politica dell'Istituto riguardo all'uso consapevole della Rete e delle TIC
- 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 alunni;
- promuovere comportamenti sicuri, la sicurezza online e assicurare la protezione degli alunni e delle alunne durante le attività che si eseguono insieme.

Al fine di condividere regole comuni per l'utilizzo sicuro di Internet sia a casa che a scuola, i genitori e/o tutori devono:

- prestare la massima attenzione ai principi e alle regole contenute nell'ePolicy;
- impegnarsi a farle rispettare ai propri figli anche in ambito domestico, assistendo i minori nel momento dell'utilizzo della rete e poi ponendo in atto tutti i sistemi di sicurezza che aiutino a diminuire il rischio di imbattersi in materiale indesiderato (control parental).

La scuola promuove eventi e incontri informativi e formativi durante l'anno scolastico sulle tematiche dell'ePolicy, rivolti a tutto il personale, agli alunni e ai loro genitori, tra cui:

- partecipazione all'evento "Safety Internet Day"
- incontri con esperti esterni e con la Polizia Postale sul tema "Bullismo, Cyberbullismo e Sicurezza in rete".

Il documento ePolicy è uno strumento efficace per la tutela degli alunni e delle alunne, per cui è utile condividere le regole per un uso consapevole e sicuro di Internet anche con le organizzazioni/associazioni extrascolastiche e gli esperti esterni chiamati, a vario titolo, per la realizzazione di progetti ed attività educative. A tal fine la scuola, oltre ai regolamenti e alle informative sulla privacy, elaborerà un'informativa sintetica sull'ePolicy, comprensiva delle azioni e delle procedure di segnalazione, da condividere con tutte le figure che operano con studenti e studentesse, per tutelare gli alunni e le alunne, ma anche per porre in essere nuove modalità per rilevare, limitare e contrastare possibili pericoli legati a condotte educative non professionali e fornire procedure di segnalazione da seguire anche per i professionisti e le organizzazioni esterne. Questo perché è importante garantire che tutti i soggetti esterni che erogano attività in ambito scolastico siano sensibilizzati e resi consapevoli dei rischi online che possono correre gli alunni e le alunne e dei comportamenti corretti che devono adottare a scuola.

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

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

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

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

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

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

Il documento E-policy, dopo l'approvazione al Collegio dei Docenti, verrà condiviso e comunicato a tutto il personale scolastico, agli alunni e ai genitori, attraverso:

- la pubblicazione del documento sul sito web della scuola;
- il Patto di Corresponsabilità, che viene sottoscritto dalle famiglie all'inizio dell'anno scolastico.

Il personale scolastico, gli alunni e i genitori verranno informati, attraverso l'ePolicy, del fatto che, accedendo alla rete Internet utilizzando i PC dell'istituzione scolastica, sono monitorati e che, attraverso il PROXY, si può risalire al singolo utente registrato.

Essi, inoltre, verranno supportati nell'uso della rete, sulla sicurezza, sulle regole da rispettare in rete e nell'uso di ogni dispositivo digitale, attraverso incontri informativi, formativi e riunioni istituzionali.

L'elenco delle regole per la sicurezza on-line verrà affisso in tutte le aule e nei laboratori con accesso a Internet.

Nello specifico, il documento verrà condiviso con:

- gli alunni/e per dare loro delle regole di sicurezza circa il comportamento da tenere a scuola e nei contesti extrascolastici; dare loro elementi per poter riconoscere e quindi prevenire comportamenti a rischio sia personali che dei/delle propri/e compagni/e;
- il personale scolastico per dare un'adeguata informazione/formazione sull'uso sicuro e responsabile di Internet, sull'uso corretto dei dispostivi e della Rete in linea anche con il codice di comportamento dei pubblici dipendenti;
- i genitori pubblicandolo sul sito web della scuola, nonché tramite momenti di informazione specifici e durante gli incontri scuola-famiglia per dare loro suggerimenti e indicazioni per

l'uso sicuro delle tecnologie digitali e di internet anche a casa.

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.

La scuola deve gestire le infrazioni all'E-policy attraverso azioni educative valutando i gradi di gravità di eventuali violazioni e analizzando i rischi connessi ad un uso poco consapevole delle tecnologie digitali.

Disciplina degli alunni

Le infrazioni in cui è probabile che gli alunni possano incorrere a scuola nell'utilizzo della rete Internet, sono le seguenti:

- la condivisione online di immagini, file audio o video di compagni/e senza il loro consenso o che li ritraggono in pose offensive e denigratorie;
- la condivisione di scatti intimi e a sfondo sessuale; la condivisione di dati personali; l'invio di immagini o video volti all'esclusione di compagni/e;
- la comunicazione incauta e senza permesso con sconosciuti;
- collegamento a siti web non indicati dai docenti.

In tali casi, è molto importante intervenire su tutto il contesto classe con attività specifiche educative e di sensibilizzazione, allo scopo di promuovere una maggior consapevolezza circa l'utilizzo delle TIC e di Internet. È opportuno, inoltre, valutare la natura e la gravità di quanto accaduto. Sono previsti, da parte dei docenti, provvedimenti "disciplinari" proporzionati all'età e alla gravità del comportamento, quali: il richiamo verbale, il richiamo scritto con annotazione sul diario, la convocazione dei genitori da parte degli insegnanti e da parte del Dirigente scolastico. Contestualmente sono previsti interventi di carattere educativo, 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, promozione di rapporti amicali, della conoscenza e della gestione delle emozioni (con il supporto psicologico all'alunno/a). In presenza di situazioni e/o episodi gravi, il Dirigente Scolastico provvederà alle opportune segnalazioni alle autorità competenti (Polizia Postale).

Disciplina del personale scolastico

Le potenziali infrazioni in cui è possibile che il personale scolastico e in particolare i docenti possono

incorrere nell'utilizzo delle tecnologie digitali e di internet sono le seguenti:

- utilizzo delle tecnologie e dei servizi della scuola, di uso comune con gli alunni, non connessi alle attività di insegnamento o al profilo professionale, anche tramite l'installazione di software o il salvataggio di materiali non idonei o non consentiti dalla legge;
- uso improprio dei device e della Rete;
- trattamento dei dati personali, comuni e sensibili degli alunni, non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi;
- diffusione delle password assegnate e una custodia non adeguata degli strumenti e degli accessi di cui possono approfittare terzi;
- una carente istruzione preventiva degli alunni sull'utilizzazione corretta e responsabile delle tecnologie digitali e di internet;
- vigilanza elusa degli alunni che può favorire un utilizzo non autorizzato delle TIC;
- insufficienti interventi di segnalazione ai genitori, al Dirigente scolastico, all'Animatore digitale di condotte improprie dei propri alunni/e.

Disciplina dei genitori

In considerazione dell'età degli alunni e della loro dipendenza dagli adulti, anche alcune condotte dei genitori possono favorire o meno l'uso corretto e responsabile delle TIC da parte degli alunni a scuola. Alcune famiglie sottovalutano i rischi a cui vanno incontro i propri figli e permettono loro di navigare in rete senza nessun controllo e di:

- rimanere a casa da soli utilizzando il PC;
- utilizzare il PC in una stanza o in un posto non visibile a tutti;
- utilizzare lo smartphone per navigare, in piena autonomia, sul web;
- utilizzare il PC in comune con gli adulti che possono conservare in memoria materiali non idonei;
- utilizzare il cellulare o lo smartphone in comune con gli adulti, che possono conservare in memoria indirizzi o contenuti non idonei.

I genitori degli alunni possono essere convocati a scuola per concordare misure educative diverse oppure essere sanzionabili a norma di legge in base alla gravità dei comportamenti dei loro figli, se dovessero risultare pericolosi per sé e/o dannosi per gli altri.

1.6 - Integrazione dell'ePolicy con Regolamenti esistenti

Il Regolamento dell'Istituto Scolastico viene aggiornato con specifici riferimenti all'E-policy, così come anche il Patto di Corresponsabilità, in coerenza con le Linee Guida Miur e le indicazioni normative generali sui temi in oggetto.

Il documento ePolicy si integra con gli obiettivi del PTOF, del PNSD e con i seguenti regolamenti in vigore nel nostro Istituto:

- Regolamento di Istituto
- Regolamento per l'utilizzo dei laboratori multimediali
- Patto di corresponsabilità.

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 monitoraggio della ePolicy dovrà prevedere la valutazione della sua efficacia in riferimento alle competenze digitali e all'uso delle TIC, alla prevenzione e gestioni dei rischi online etc…).

Il monitoraggio sarà curato da un docente referente nominato dal Dirigente scolastico con la collaborazione dell'Animatore digitale, dal referente del Bullismo e Cyberbullismo, attraverso questionari.
Esso verrà fatto all'inizio di ogni anno scolastico insieme alla revisione del PTOF e alla fine dell'anno scolastico, per rilevare la situazione delle classi, in relazione all'uso sicuro e responsabile delle tecnologie digitali e di internet. Il monitoraggio sarà rivolto anche agli insegnanti, al fine di valutare l'impatto della e-Policy e la necessità di eventuali miglioramenti.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i docenti dell'Istituto per la stesura finale dell'ePolicy.
- Organizzare incontri per la consultazione degli studenti/studentesse sui temi dell'ePolicy per cui si evidenzia la necessità di regolamentare azioni e

comportamenti.
- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i genitori dell'Istituto per la stesura finale dell'ePolicy.
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto agli studenti
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai docenti
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai genitori
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto agli studenti
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai docenti
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai genitori

Azioni da svolgere nei prossimi 3 anni:

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

Capitolo 2 - Formazione e curricolo

2.1. Curricolo sulle competenze digitali per gli studenti

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

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

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

La competenza digitale consiste nel saper utilizzare con dimestichezza e spirito critico le tecnologie dell'informazione e della comunicazione. Essa è supportata da abilità di base nell'uso delle TIC per reperire, valutare, conservare, produrre, presentare e scambiare informazioni per comunicare e partecipare a reti collaborative tramite Internet. Per tal motivo la scuola deve portare avanti percorsi volti all'acquisizione di tali competenze, per educare gli alunni e le alunne verso un uso consapevole e responsabile delle tecnologie digitali. Le competenze digitali, rientrano tra le otto competenze chiave di cittadinanza della Raccomandazione Europea, ritenute utili per l'apprendimento permanente. Anche nelle Indicazioni Nazionali e successivamente nelle Indicazioni del PNSD esse vengono ritenute come competenze trasversali a tutte le discipline, in quanto richiamano diverse dimensioni sulle quali sarà possibile lavorare in classe, in un'ottica che integra la dimensione tecnologica con quella cognitiva ed etica (Calvani, Fini e Ranieri 2009):

- dimensione tecnologica: fa riferimento alle potenzialità delle tecnologie digitali come strumenti per la risoluzione di problemi della vita quotidiana;
- dimensione cognitiva: fa riferimento alla capacità di cercare, usare e creare in modo critico le informazioni condivise in Rete, valutandone credibilità e affidabilità;

- dimensione etica e sociale: fa riferimento alla capacità di gestire la propria privacy e quella degli altri in modo sicuro, e di usare le tecnologie digitali nel rispetto degli altri. Ma anche allo sviluppo di abilità socio-comunicative per maturare una maggiore consapevolezza sui nostri doveri nei riguardi di coloro con cui comunichiamo online.

Queste competenze si possono raggiungere attraverso la progettazione di un curricolo digitale, trasversale alle varie discipline che permetta agli alunni, di utilizzare in maniera consapevole e responsabile le più comuni tecnologie dell'informazione e della comunicazione. La nostra scuola, in coerenza con quanto affermato e in coerenza con il PTOF 2020/21 e il PNSD (Piano Nazionale Scuola Digitale), nel curricolo verticale e in quello di educazione civica attiverà percorsi formativi per acquisire i seguenti obiettivi finalizzati a:

- Promuovere un uso consapevole delle nuove tecnologie;
- Navigare, ricercare e filtrare dati, informazioni e contenuti digitali;
- Saper riconoscere i rischi e sapersi difendere da contenuti dannosi e pericolosi in Rete (app, giochi online, siti non adatti ai minori);
- Saper interagire con gli altri attraverso le tecnologie digitali;
- Essere consapevoli nella condivisione delle informazioni in Rete;
- Distinguere la differenza tra realtà virtuale e reale;
- Collaborare adeguatamente con gli altri attraverso le tecnologie digitali;
- Conoscere le "Netiquette", ovvero le norme di comportamento online;
- Creare e modificare contenuti digitali in diversi formati per esprimersi attraverso mezzi digitali;
- Capire come il copyright e le licenze si applicano ai dati, alle informazioni e ai contenuti digitali;
- Proteggere i dati personali e la privacy negli ambienti digitali. Capire come utilizzare e condividere informazioni personali proteggendo se stessi e gli altri dai danni.

Questi obiettivi verranno acquisiti in modo trasversale attraverso percorsi didattici disciplinari e interdisciplinari.

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 formazione costituisce uno strumento fondamentale per lo sviluppo professionale dei docenti e non docenti. La legge 107 definisce la formazione del personale della scuola come “obbligatoria, permanente e strategica” e la riconosce come opportunità di effettivo sviluppo e crescita professionale. Ai docenti spetta, quindi, nel proprio codice di comportamento professionale, la cura della propria formazione come scelta personale prima che come obbligo.
Le competenze che ogni docente deve possedere sono diverse ed integrate, fra queste anche quelle di tipo digitale. Le TIC, infatti, devono essere usate dagli insegnanti ad integrazione della didattica al fine di:

- progettare, sviluppare, utilizzare, gestire e valutare i processi di insegnamento e apprendimento di tutti gli alunni della classe, anche di quelli con disabilità

- promuovere la condivisione di buone pratiche per un uso consapevole e sicuro delle risorse digitali (Legge 107/2015)

È su tali premesse che il nostro Istituto favorisce la partecipazione dei Docenti a percorsi formativi centrati sull’uso delle Nuove Tecnologie, degli ambienti di apprendimento eLearning e di alcuni applicativi, per creare Learning Objects e attivare una didattica laboratoriale integrata.

Per l’attuazione degli interventi formativi, il nostro Istituto si avvale di corsi organizzati dal MIUR, dall’USR, dalla rete territoriale e ha aderito al progetto “Generazioni Connesse”, e a corsi gestiti da associazioni per la tutela dei diritti dei minori. Si avvale anche di corsi interni su specifiche aree tematiche, secondo quanto previsto dal PNSD, tenuti dall’Animatore Digitale. Quest’anno, per realizzare le azioni relative al PNSD, è stato elaborato, a cura dell’Animatore Digitale, il piano della formazione progettato, a partire dai bisogni formativi dei docenti, e finalizzato a far acquisire competenze su diversi ambiti tra cui quelle digitali. L’obiettivo principale è quello di far utilizzare le TIC, in sicurezza, integrandole nella didattica, per rendere gli apprendimenti motivanti, coinvolgenti ed inclusivi. Nello stesso progetto sono stati previsti anche corsi di formazione sulla Didattica a distanza. La progettazione degli interventi formativi ha come punto di partenza l’individuazione di competenze digitali che ogni docente oggi dovrebbe avere, tenendo conto del DigComp (il quadro di riferimento per le competenze digitali dei cittadini).

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.

Nel nostro Istituto vengono attivati percorsi formativi specifici finalizzati non solo all'uso responsabile e sicuro della Rete ma anche a conoscere e prevenire i rischi online. Questo sarà possibile tramite specifici e adeguati momenti di aggiornamento che verranno organizzati con il supporto della rete scolastica territoriale (Scuole Polo, USR) e di corsi interni con la collaborazione dell'Animatore Digitale e del referente del Bullismo e Cyberbullismo. A tal fine il nostro Istituto ha aderito al progetto "Generazioni Connesse" e l'Animatore Digitale ha iscritto molti docenti per partecipare ai corsi di formazione sui temi previsti in piattaforma (https://www.generazioniconnesse.it/piattaforma/). Nel corso dell'anno scolastico il nostro Istituto partecipa al "**Safer Internet Day**" e vengono organizzati eventi destinati ai docenti, ai genitori e alunni relativi al "Bullismo, Cyberbullismo e sicurezza in rete", per sensibilizzare la comunità scolastica sui rischi della rete e sull'uso corretto delle Nuove Tecnologie. Per informare il personale scolastico e extrascolastico, è stato predisposto sul sito web della scuola il link al progetto "www.generazioniconnesse.it" dove trovare ulteriori approfondimenti, materiali informativi e strumenti didattici utili da usare con gli alunni/e, per ciascun grado di scuola. Sarà predisposta, inoltre, sul sito web della scuola, una sezione specifica dove verranno inseriti materiali formativi per l'aggiornamento dei Docenti, sull'utilizzo consapevole e sicuro della rete Internet.

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.

Si avrà cura di sensibilizzare i genitori sulle tematiche relative alle TIC, della sicurezza in rete e per informarli sulle situazioni di rischio on-line. A tal fine saranno previsti degli incontri formativi tra docenti e genitori per condividere il materiale informativo. Inoltre, si organizzeranno, nei prossimi

anni scolastici, incontri formativi con la Polizia Postale per i genitori, alunni e docenti sui temi del Cyberbullismo e sulla Sicurezza online. Per rendere partecipi le famiglie del documento di ePolicy e del piano d'azione dell'Istituto, verranno organizzati incontri con i genitori per informarli sulle condotte che si dovranno adottare a scuola e, in generale, offrire loro consigli da mettere in pratica con i propri figli. Saranno informati, infatti, sulle misure di restrizione da attivare in rete per far navigare i propri figli in sicurezza e saranno sensibilizzati a consultare il portale www.generazioniconnesse.it, dove potranno trovare materiale, guide, video per un maggior approfondimento sulla sicurezza online.

L'ePolicy verrà presentato in tutti i Consigli di classe e di Interclasse e verrà pubblicato anche sul sito Web della scuola, per far conoscere alle famiglie il regolamento sull'utilizzo delle nuove tecnologie all'interno dell'Istituto e per prevenire i rischi legati ad un utilizzo scorretto di Internet.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2019/2020)

Scegliere almeno 1 di queste azioni

- Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Coinvolgere una rappresentanza dei genitori per individuare i temi di maggiore interesse nell'ambito dell'educazione alla cittadinanza digitale.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare incontri con esperti per i docenti sulle competenze digitali.
- Organizzare incontri con esperti per i genitori sull'educazione alla cittadinanza digitale.

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

Scegliere almeno 1 di queste azioni

- Effettuare un’analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.
- Effettuare un’analisi del fabbisogno formativo del corpo docente sull’utilizzo e l’integrazione delle TIC nella didattica.
- Effettuare un’analisi del fabbisogno formativo del corpo docente sull’utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Coinvolgere una rappresentanza dei genitori per individuare i temi di maggiore interesse nell’ambito dell’educazione alla cittadinanza digitale.
- Organizzare e promuovere per il corpo docente incontri formativi sull’utilizzo e l’integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi sull’utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare incontri con esperti per i docenti sulle competenze digitali.
- Organizzare incontri con esperti per i genitori sull’educazione alla cittadinanza digitale.

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

3.1 - Protezione dei dati personali

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

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

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

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

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

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

personali.

La protezione dei dati personali è un diritto fondamentale dell'individuo ai sensi della Carta dei diritti fondamentali dell'Unione europea (art. 8). Oggi le scuole hanno 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 e hanno l'obbligo di garantire la tutela della privacy, dei dati personali dei soggetti coinvolti nel processo educativo, con particolare attenzione ai soggetti minorenni. Tutto il personale scolastico e amministrativo sono incaricati del trattamento dei dati personali nel rispetto delle norme previste in materia per fini burocratici e organizzativi. Esso riceve istruzioni particolareggiate applicabili al trattamento di dati personali, ai fini della protezione e sicurezza degli stessi. Utilizzare il digitale comporta una responsabilità. Oggi l'uso delle Tecnologie digitali a scopo didattico, la condivisione online di contenuti didattici, l'uso del registro elettronico e delle piattaforme eLearning e/o gruppi WhatsApp 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. Questo perché la velocità, l'immediatezza con cui si risponde ai messaggi o si condividono foto o video, può mettere a rischio la sicurezza dei soggetti coinvolti e in particolar modo se questi sono minori. La nostra scuola, per garantire la tutela della privacy e il diritto alla riservatezza dei soggetti coinvolti nel processo educativo, utilizza i dati personali necessari al perseguimento di specifiche finalità istituzionali e rende noto alle famiglie, attraverso un'adeguata informativa, quali dati raccolgono e come li utilizzano; chiede, inoltre, l'autorizzazione all'utilizzo dei dati personali degli alunni mediante liberatoria, conforme alla normativa vigente, in materia di protezione dei dati. Per quanto riguarda i docenti, ognuno è responsabile delle proprie credenziali di accesso al registro elettronico e viene raccomandato sempre di:

- non salvare mai le proprie password
- effettuare il logout dalle proprie caselle di posta elettronica
- utilizzare password sicure e cambiarle ogni tre mesi
- non condividere numeri di telefono personali o indirizzi di posta elettronica privati con i genitori e alunni

La scuola cercherà di:

- utilizzare fotografie di gruppo piuttosto che foto di singoli
- non pubblicare i nomi completi degli alunni sul sito web, in particolare se in associazione con le loro fotografie.

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.

Il diritto di accesso a Internet è 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". A tal fine la nostra scuola garantisce questo diritto e dispone di una rete LAN per gli uffici amministrativi e di una rete per la didattica, mantenendo quindi separate le reti didattica e segreteria. Ci si connette a Internet tramite l'ADSL, attraverso la rete LAN e la rete Wi-fi; il firewall e il PROXY garantiscono un buon livello di sicurezza on-line. L'accesso a Internet è possibile sia nelle classe che nei laboratori multimediali. L'accesso è per tutti schermato da filtri che impediscono il collegamento a siti appartenenti alla black list e che consentono, invece, il collegamento solo a siti sicuri e idonei alla didattica tramite l'utilizzo di white list per la navigazione, secondo le impostazioni date dal responsabile tecnico che, periodicamente, provvede alla manutenzione e all'aggiornamento del sistema informatico dei laboratori e delle aule. Tutti i PC sono forniti di antivirus. Le apparecchiature presenti nella scuola sono un patrimonio comune, quindi, vanno utilizzate con il massimo rispetto senza modificare lo sfondo del desktop, la risoluzione del video, le impostazioni, la configurazione originale

dell'hardware e le connessioni di rete. L'accesso ai PC dei laboratori multimediali, è consentito al personale docente e agli alunni, mentre l'accesso al PC delle aule è consentito solo ai docenti. In ogni PC sono stati creati gli account, uno Amministratore e gli altri standard, ai quali si accede con password assegnata da parte della F.S. Area 2 "Sostegno al lavoro dei docenti - Coordinamento e gestione delle tecnologie informatiche e della comunicazione".

I docenti che accedono ai laboratori multimediali, registrano il proprio accesso, scrivendo su un registro la data e l'orario di utilizzo del laboratorio. In ogni laboratorio multimediale c'è un server che è la postazione di lavoro per il docente e ci sono i PC per gli alunni. In tutte le postazioni, ci sono due account, uno per i docenti e uno per gli alunni. Nell'account docente si accede tramite password. Dal server il docente può controllare le postazioni degli alunni tramite il software della rete didattica. I file creati vengono salvati, dai docenti interessati e/o dagli alunni nella cartella per la propria classe, in documenti oppure sui supporti rimovibili personali. Tutti i dispositivi in uso nella scuola, sia delle classi che dei laboratori sono muniti di antivirus. Il responsabile del laboratorio informatico, che attualmente coincide con la figura della F.S. Area 2 "Sostegno al lavoro dei docenti - Coordinamento e gestione delle tecnologie informatiche e della comunicazione", periodicamente provvede alla manutenzione del laboratorio informatico richiedendo, ove necessario, anche l'intervento di tecnici esterni.

Gestione accessi (password, backup, etc...)

La rete possiede un sistema di navigazione che viene gestita da un server PROXY, un server che si interpone nel flusso di comunicazione fra un computer e un sito Internet. Esso controlla la navigazione degli accessi di tutti i PC collegati. Ad ogni PC si accede tramite password che vengono aggiornate periodicamente. Le postazioni dei lboratori hanno due account, uno per il docente, il quale accede tramite password, e uno per gli alunni. Il PC collegato alla LIM, di ogni aula, viene utilizzato solo dal docente, il quale accede tramite password. Ogni docente ha una password personale per accedere al registro ARGO Nuovo Didup. Le operazioni di configurazione e di ripristino dei PC dei laboratori e delle classi viene fatto dal Responsabile dell'Area Tecnologica e dal tecnico esterno. Le operazioni di backup vengono effettuati solo nei PC degli uffici di segreteria. È possibile effettuare installazioni e aggiornamenti di software solo tramite la password di amministratore, fornita al responsabile dell'area tecnologica (Animatore Digitale).

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.

Gli strumenti di comunicazione online, utilizzati a scuola, integrando quelli più tradizionali e che rendono lo scambio comunicativo, collaborativo e maggiormente interattivo sono diversi. Nella nostra scuola, come strumento di comunicazione online, abbiamo utilizzato, in alcune classi, Edmodo. In questo ambiente virtuale, gli alunni hanno potuto comunicare, inserire attività, ascoltare file audio e video. Ultimamente è stata adottata la piattaforma Microsoft 365 e l'App Microsoft Teams, lo strumento unificato di comunicazione e collaborazione che offre diverse funzionalità e permette di avviare conferenze video, effettuare e ricevere chiamate con gruppi interni ed esterni, condividere e modificare agevolmente file in tempo reale utilizzando le App di Word, PowerPoint ed Excel. A TEAMS, sia i docenti che gli alunni, possono accedere inserendo le proprie credenziali. In questa piattaforma i docenti potranno creare videolezioni, classi virtuali per discipline e/o per classi, e gli alunni potrà partecipare, comunicare e interagire, in modo consapevole, alle lezioni.

TEAMS per noi rappresenterà un'opportunità significativa per coinvolgere maggiormente gli alunni utilizzando diversi linguaggi (scrittura, immagini, video etc…). Grazie agli strumenti di comunicazione online potremo usufruire dell'interattività del mezzo, superare le barriere spazio-temporali, usare un linguaggio multimediale, ipertestuale e accattivante, promuovere la partecipazione e il coinvolgimento dei diversi attori in gioco nel processo educativo.

L'istituzione scolastica ha anche una pagina Facebook con il proprio profilo che viene gestita dall'Animatore Digitale sotto la supervisione del Dirigente. Ha, inoltre, un canale You Tube, dove vengono pubblicati video e attività realizzate dagli alunni utilizzando musiche e file audio con licenze di Creative Commons per non violare il copyright. All'inizio di ogni anno scolastico viene chiesto alle famiglie di firmare una liberatoria relativa alla pubblicazione di foto in immagini e video prodotti dalla scuola.

Per la messaggistica tra docenti e docenti/genitori, viene utilizzato l'applicativo online WhatsApp sempre rispettando e ricordando il "diritto alla disconnessione"; esso, infatti, non viene utilizzato in orario di servizio.

Sito web della scuola

Il nostro Istituto possiede un sito istituzionale www.circolo2sancataldo.edu.it che viene gestito dall'Animatore Digitale che coincide con la F.S. Area 2 "Coordinamento e gestione delle tecnologie informatiche e della comunicazione. Esso viene aggiornato costantemente con l'inserimento dei contenuti e delle news. Il sito utilizza il protocollo HTTPS (l'Hypertext Transfer Protocol Secure, un protocollo per la comunicazione su Internet che protegge l'integrità e la riservatezza dei dati scambiati online). Nel sito ci sono diverse sezioni e contenuti utili alle famiglie:

- Avvisi

- Regolamenti

- PTOF

- Modulistica

- Progetti

- link alla piattaforma “Generazioni Connesse”

- Sicurezza, etc…

I dati di tipo economico-amministrativo vengono inseriti dagli addetti del personale di Segreteria. L’inserimento dei contenuti vengono pubblicati, sotto la supervisione del Dirigente che ne valuta la sicurezza e l’adeguatezza sotto i diversi profili dell’accessibilità, della pertinenza dei contenuti, del rispetto della privacy e secondo il regolamento del “Codice in materia della protezione dei dati personali”. Nel sito è stato inserito il collegamento al registro elettronico ARGO.
L’Istituto attualmente ha anche un Blog, dal titolo ”Security in rete”, che intende offrire all’utenza un percorso sulle tematiche della sicurezza on line e sull’uso delle tecnologie nella didattica in modo responsabile e consapevole. Tra gli strumenti di comunicazione, come detto precedentemente, la nostra scuola ultimamente ha adottato la piattaforma Microsoft 365 Education e Teams, che verrà utilizzata per la DDI.

Registro elettronico

Il registro elettronico adottato dalla nostra scuola è Argo Nuovo Didup, nel quale possono accedere sia i Docenti che i genitori tramite password dedicate e personali. I Docenti registrano le assenze, le attività, le valutazioni e le osservazioni. I genitori accedono tramite Argo famiglie per visualizzare le attività, i compiti assegnati, le valutazioni e anche le comunicazioni. Argo permette anche di gestire la comunicazione con le famiglie, le quali attraverso di esso possono visualizzare molte informazioni utili, interagendo con la scuola, su:

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

Ultimamente il registro è stato aggiornato e migliorato in alcune sezioni e, attraverso la bacheca di Nuovo Didup, adesso i docenti possono condividere ai genitori le lezioni asincrone. Esso, va ancora migliorato e arricchito di altri servizi, come per esempio il servizio online interattivo tra docenti e genitori. Tale servizio potrebbe essere molto utile per creare moduli, questionari, sondaggi e condividerli online e per ricevere i dati in modo istantaneo senza ricorrere a piattaforme esterne.

E-mail

L’account di posta elettronica è quello istituzionale utilizzato ordinariamente dagli uffici amministrativi, sia per la posta in ingresso che in uscita. L’eventuale invio o ricevimento di posta a scopi didattici avverrebbe solo su autorizzazione del Dirigente scolastico e operativamente sarebbe svolto dall’Assistente Amministrativo addetto. La posta elettronica è protetta da antivirus e quella certificata anche dall’antispam. Tutti i docenti possiedono una mail professionale e una privata.
La scuola ha anche un account email istituzionale @secondocircolosancataldo.onmicrosoft.com con il quale genera le credenziali ai docenti e agli alunni per utilizzare la didattica a distanza.

3.4 - Strumentazione personale

I dispositivi tecnologici sono parte integrante della vita personale di ciascuno, compresa quella degli/lle studenti/esse e dei docenti (oltre che di tutte le figure professionali che a vario titolo sono inseriti nel mondo della scuola), ed influenzano necessariamente anche la didattica e gli stili di apprendimento. Comprendere il loro utilizzo e le loro potenzialità innovative, diventa di cruciale importanza, anche considerando il quadro di indirizzo normativo esistente e le azioni programmatiche, fra queste il Progetto Generazioni Connesse e il più ampio PNSD.

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

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

La strumentazione tecnologica personale, in riferimento al PNSD, può essere utilizzata dai docenti nella didattica, per stimolare gli alunni a partecipare maggiormente alle attività didattiche. Questa possibilità viene annullata dalla normativa vigente posta a tutela della privacy, il divieto di utilizzo di telefoni cellulari o di altri dispositivi elettronici nelle comunità scolastiche allo scopo di acquisire e/o divulgare immagini, filmati o registrazioni vocali. In riferimento a tale norma, nella nostra Istituzione non è consentito l'utilizzo dello smartphone, durante lo svolgimento delle attività didattiche, tranne se richiesto dai docenti per le attività didattiche finalizzate ad attuare il BYOD (Bring Your Own Device) a scuola. L'uso viene consentito solo per scopi prettamente didattici, sotto il controllo e la responsabilità del docente che pianifica l'attività didattica.

A tal fine, gli smartphone e i tablet personali potranno essere utilizzati solo per eseguire attività disciplinari progettate e finalizzate all'acquisizione di obiettivi didattici. Pertanto si potranno utilizzare per rispondere a questionari, a quiz, sondaggi o per realizzare produzioni digitali, sempre sotto la guida e il controllo costante dell'insegnante.

Nel caso in cui gli alunni debbano comunicare con la famiglia, durante l'orario scolastico, possono utilizzare la linea fissa della scuola chiedendo al collaboratore. Nel processo educativo e didattico, si va quindi verso la responsabilizzazione dei soggetti dove l'utilizzo delle tecnologie e dei dispositivi anche personali va mediato e calibrato sviluppando un pensiero critico. Educare alla cittadinanza digitale è un dovere per la scuola. Formare i futuri cittadini significa educare alla partecipazione responsabile, all'uso critico delle tecnologie, alla consapevolezza e alla costruzione delle proprie competenze in un mondo sempre più connesso. In tale ottica, verranno integrati i Regolamenti già esistenti per disciplinare l'utilizzo delle TIC all'interno della scuola, dotando la scuola di filtri per prevenire i rischi durante la navigazione online e stabilire procedure specifiche per rilevare e gestire le diverse problematiche. I docenti, durante le ore delle lezioni, possono fruire di altri device elettronici personali solo a scopo didattico ed integrativo di quelli scolastici e possono utilizzare i dispositivi in dotazione della scuola esclusivamente per fini didattici. L'uso incauto dei dispositivi comuni può essere addebitato al responsabile del danno attraverso la

tracciabilità dell'accesso. L'utilizzo della rete WI-FI sarà autorizzato, previa richiesta, dal D.S. che ne valuterà la coerenza con gli scopi didattici garantiti dal richiedente. Il collegamento di qualsiasi dispositivo potrà essere monitorato e controllato attraverso software di gestione della rete. Se a scuola vengono utilizzati dispositivi di archiviazione esterna di proprietà personale (chiavette usb, hard disk portatili) è opportuno controllare preventivamente che essi siano esenti da virus per evitare di danneggiare le attrezzature comuni. Durante l'orario di servizio al personale scolastico è consentito l'utilizzo del cellulare solo per comunicazioni personali di carattere urgente, e solo a condizione che non impedisca il normale svolgimento dei propri compiti.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2019/2020).

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.*

I rischi effettivi che gli alunni possono incontrare derivano dall'utilizzo dei PC. Infatti, può accadere che, eludendo la vigilanza degli insegnanti, gli alunni si colleghino a siti poco sicuri per scaricare immagini, foto e video con contenuti violenti e non adatti alla loro età, a videogiochi diseducativi con il rischio di essere contattati da adulti con intenzioni malevoli, o si colleghino per comunicare e chattare con sconosciuti con il rischio di adescamento online (grooming), o per inviare e/o ricevere messaggi di molestia e minacce da coetanei (cyberbullismo). Per evitare questo è necessario e indispensabile che gli alunni acquisiscano quelle competenze e capacità adeguate per utilizzare in modo consapevole, sfruttando le potenzialità delle Nuove Tecnologie e sapendo gestire le implicazioni.A tal fine nel nostro Istituto abbiamo attivato percorsi formativi di prevenzione e

formiamo gli alunni sulla sicurezza online per evitare i rischi legati all'uso del digitale. Abbiamo rivisto il curricolo verticale integrandolo di competenze, contenuti sui temi legati all'utilizzo sicuro delle TIC e della rete, per tutte le classi della scuola. Si intende, pertanto, di mettere in campo interventi di Sensibilizzazione e Prevenzione in modo da fornire non solo le informazioni necessarie ma anche illustrando le soluzioni e i comportamenti da adottare. In questo percorso formativo, la scuola si avvale della collaborazione di enti, associazioni e della Polizia Postale, che operano sul territorio, per realizzare incontri rivolti agli alunni, ai docenti e alle famiglie, con l'intento di fornire elementi utili per prevenire, gestire i problemi relativi alla sicurezza informatica e contrastare il bullismo e il cyberbullismo.

Di seguito le linee guida da rispettare per l'uso positivo delle tecnologie digitali e per prevenire eventuali rischi legati al loro.

Linee guida per gli alunni

- Non comunicare mai a nessuno la tua password e periodicamente va cambiata, usando numeri, lettere e caratteri speciali.
- Mantieni segreto il nome, l'indirizzo, il telefono di casa, il nome e l'indirizzo della tua scuola.
- Non inviare a nessuno fotografie tue o di tuoi amici; prima di inviare o pubblicare su un BLOG la fotografia di qualcuno, chiedi sempre il permesso.
- Chiedi sempre al tuo insegnante o ai tuoi genitori il permesso di scaricare documenti Internet.
- Chiedi sempre il permesso prima di iscriverti a qualche concorso o prima di riferire l'indirizzo della tua scuola.
- Quando sei connesso alla rete RISPETTA SEMPRE GLI ALTRI, ciò che per te è un gioco può rivelarsi offensivo per qualcun altro.
- Non rispondere alle offese e agli insulti.
- Blocca i Bulli: molti Blog e siti social network ti permettono di segnalare i cyberbulli.
- Conserva le comunicazioni offensive, ti potrebbero essere utili per dimostrare quanto ti è accaduto.
- Se ricevi materiale offensivo (e-mail, sms, video, foto, messaggi vocali) non diffonderlo: potresti essere accusato di cyberbullismo.
- Rifletti prima di inviare: ricordati che tutto ciò che invii su internet diviene pubblico e rimane per SEMPRE.
- Riferisci al tuo insegnante o ai tuoi genitori se qualcuno ti invia immagini che ti infastidiscono e non rispondere; riferisci anche al tuo insegnante o ai tuoi genitori se ti capita di trovare immagini di questo tipo su Internet.
- Se qualcuno su Internet ti chiede un incontro di persona, riferiscilo al tuo insegnante o ai tuoi genitori.
- Ricordati che le persone che incontri nella Rete sono degli estranei e non sempre sono quello che dicono di essere.
- Non è consigliabile inviare e-mail personali, perciò rivolgiti sempre al tuo insegnante prima di inviare messaggi di classe o ai tuoi genitori prima di inviare messaggi da casa.
- Non scaricare (download) o copiare materiale da Internet senza il permesso del tuo insegnante o dei tuoi genitori.
- Non caricare (upload) materiale video o fotografico nei siti web dedicati senza il permesso

del tuo insegnante o dei tuoi genitori.

Linee guida per i genitori per un uso responsabile di internet a casa

- Posizionate il computer in salone o in una stanza accessibile a tutta la famiglia.
- Evitate di lasciare le e-mail o file personali sui computer di uso comune.
- Concordate con vostro figlio le regole: quando si può usare internet e per quanto tempo.
- Inserite nel computer i filtri di protezione: prevenite lo spam, i pop-up pubblicitari, l'accesso a siti pornografici.
- Aumentate il filtro del "parental control" attraverso la sezione sicurezza in internet dal pannello di controllo; attivate il firewall (protezione contro malware) e antivirus.
- Mostratevi coinvolti: chiedete a vostro figlio di mostrarvi come funziona internet e come viene usato per scaricare e caricare compiti, lezioni, materiali didattici e per comunicare con l'insegnante.
- Incoraggiate le attività on-line di alta qualità: ricercare informazioni scientifiche e fare ricerche.
- Partecipate alle esperienze on-line: navigate insieme a vostro figlio, discutete degli eventuali problemi che si presentano.
- Spiegate a vostro figlio che la password per accedere ad alcune piattaforme è strettamente personale e non deve essere mai data ai compagni o ad altre persone.
- Stabilite ciò che ritenete inaccettabile (razzismo, violenza, linguaggio volgare, pornografia).
- Discutete sul fatto che scaricando file da siti sconosciuti c'è la possibilità di ricevere file con virus.
- Incoraggiate vostro figlio a dirvi se vedono immagini particolari o se ricevono e-mail indesiderate.
- Discutete nei dettagli le conseguenze che potranno esserci se vostro figlio visita deliberatamente siti non adatti, ma non rimproveratelo se compie azioni involontarie.
- Il modo migliore per proteggere vostro figlio è usare Internet con loro, discutere e riconoscere insieme i rischi potenziali.

Linee guida per insegnanti

- Evitate di lasciare file personali sui PC della scuola, lo spazio è di uso comune.
- Salvate sempre i vostri lavori (file) in cartelle di classe e non sul desktop.
- Discutete con gli alunni della ePolicy della scuola, dell'utilizzo consentito della rete, e degli eventuali problemi che possono verificarsi nell'applicazione delle regole relative all'uso di Internet.
- Date chiare indicazioni agli alunni su come si utilizza Internet, ed eventualmente anche la posta elettronica, e informateli che le navigazioni sono monitorate.
- Ricordate di disconnettervi dal proprio account, di uscire da tutte le sessioni di lavoro su Internet e di spegnere il computer.
- Ricordate agli alunni che la violazione consapevole della ePolicy della scuola comporta sanzioni di diverso tipo.
- Adottate provvedimenti "disciplinari" proporzionati all'età e alla gravità del comportamento.
- Adottate interventi di carattere educativo di rinforzo dei comportamenti corretti e riparativi, di ri-definizione delle regole sociali di convivenza attraverso la partecipazione consapevole e

attiva degli alunni della classe.
- Nelle situazioni psico-socio-educative particolarmente problematiche, convocate i genitori o gli esercenti la potestà per valutare con loro a quali risorse territoriali possono rivolgersi.

4.2 - Cyberbullismo: che cos'è e come prevenirlo

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

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

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

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

Il cyberbullismo è una forma di prepotenza virtuale attuata attraverso l'uso della rete Internet e delle nuove tecnologie della comunicazione. Gli studiosi infatti lo definiscono come un'azione aggressiva, intenzionale, agita da un individuo utilizzando mezzi elettronici, nei confronti di una persona, che non può difendersi. Come nel bullismo tradizionale, la vittima che viene presa di mira è percepita come più debole ed è incapace di difendersi. Il più forte assume atteggiamenti prevaricatori, diffamatori, prepotenti e vengono fatte in modo ripetuto e continuato nel tempo, nei confronti di un'altra persona percepita come più debole. Le caratteristiche tipiche del bullismo, quindi, sono l'intenzionalità, la persistenza nel tempo, l'asimmetria di potere e la natura sociale del fenomeno. Quando queste vessazioni vengono fatte online, diventano cyberbullismo.

Le caratteristiche del cyberbullismo sono:

- **L'impatto:** la diffusione di materiale nella rete Internet è incontrollabile e illimitata (anche se la situazione migliora, video e immagini potrebbero restare online e continuare a diffondersi). Essa può diventare virale e distruggere la reputazione della vittima.
- **La convinzione dell'anonimato**: chi offende online potrebbe tentare di rimanere nascosto dietro un nickname e cercare di non essere identificabile. Sentendosi protetti dall'anonimato ci si sente liberi e più forti nel compiere atti denigratori, senza il timore di essere scoperti. Ogni nostra azione online è, infatti, rintracciabile e riconducibile a noi con gli strumenti opportuni o con l'intervento della Polizia Postale.
- **L'assenza di confini spaziali:** il cyberbullismo può avvenire ovunque, invadendo anche gli spazi personali e privando l'individuo dei suoi spazirifugio. La vittima, infatti, può essere raggiungibile anche a casa e si sente impotente.
- **L'assenza di limiti temporali**: il cyberbullismo può avvenire sempre, a ogni ora del giorno e della notte.
- **L'indebolimento dell'empatia**: esistono cellule chiamate neuroni specchio che ci permettono di "leggere" gli altri quando li abbiamo di fronte, capirli e di provare emozioni simile a quelle che loro provano, proprio come se fossimo di fronte ad uno specchio. Tale sensazione è data dall'attivazione di una particolare area del cervello. Quando le interazioni avvengono prevalentemente online la funzione speciale di questi neuroni viene meno (mancando la presenza fondamentale dell'altro che è sostituito dal dispositivo). La riduzione di empatia che ne consegue può degenerare nei comportamenti noti messi in atto dai cyberbulli.
- **Il feedback non tangibile**: il cyberbullo non vede in modo diretto le reazioni della vittima e, ancora una volta, ciò riduce fortemente l'empatia e il riconoscimento del danno provocato.

Per questo il cyberbullo non è mai consapevole delle conseguenze delle proprie azioni. L'impossibilità di vedere con i propri occhi la sofferenza e umiliazione provata dalla vittima fa sì che il tutto venga percepito come "uno scherzo" divertente a cui partecipare, di cui ridere o a cui essere indifferenti. Inoltre, il cyberbullismo non lascia segni fisici evidenti sulla vittima e si consuma in un contesto virtuale che spesso viene percepito dai ragazzi come non "reale", come un mondo ludico a sé stante.I giovani hanno anche altre convinzioni e percepiscono la Rete come:

- uno spazio online dove non ci sono regole e norme da rispettare

- il luogo virtuale per eccellenza in cui mettersi in gioco “fingendo di essere ciò che non si è” per sperimentare nuove forme di identità e comportamento

- un luogo di simulazione e giochi di ruolo: “la vita sullo schermo”, dove tutti i comportamenti messi in atto online vengono percepiti solo come un gioco

- **Diffusione di responsabilità:** tutti quelli che partecipano anche solo con un like o un commento diventano, di fatto, corresponsabili delle azioni del cyberbullo facendo accrescere la portata dell’azione; mettere un “like” su un social network, commentare o condividere una foto o un video che prende di mira qualcuno o tacere pur sapendo, mette ragazzi e ragazze nella condizione di avere una responsabilità.

Gli atti di cyberbullismo si possono suddividere in due gruppi:

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

Nel nostro Istituto è stata individuata una referente che, insieme al gruppo di lavoro, ha il compito di coordinare le iniziative di prevenzione e di contrasto del cyberbullismo. Molti docenti si sono iscritti ai corsi di formazione della piattaforma Generazioni Connesse. Gli episodi di bullismo e cyberbullismo non coinvolgono solo il minorenne, ma le responsabilità potranno ricadere anche sui genitori (culpa in educando), sui docenti e la scuola (culpa in vigilando – culpa in organizzando). A tal proposito, la scuola adotta l’ePolicy e mette in atto degli interventi per sensibilizzare alunni ad un uso responsabile e consapevole della rete, al fine di tutelarsi e tutelare i compagni da abusi e comportamenti rischiosi e/o non rispettosi e, al contempo, valorizzare le potenzialità delle TIC nella collaborazione e nella promozione delle diversità e della crescita formativa.

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

Il fenomeno di “incitamento all’odio” o “discorso d’odio”, indica discorsi (post, immagini, commenti etc.) e pratiche (non solo online) che esprimono odio e intolleranza verso un gruppo o una persona (identificate come appartenente a un gruppo o categoria) e che rischiano di provocare reazioni violente, a catena. Più ampiamente il termine “hate speech” indica un’offesa fondata su una qualsiasi discriminazione (razziale, etnica, religiosa, di genere o di orientamento sessuale, di disabilità, eccetera) ai danni di una persona o di un gruppo.

Tale fenomeno, purtroppo, è sempre più diffuso ed estremamente importante affrontarlo

anche a livello educativo e scolastico con l'obiettivo di:

- fornire agli studenti gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di hate speech, in particolare legati alla razza, al genere, all'orientamento sessuale, alla disabilità;
- promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network;
- favorire una presa di parola consapevole e costruttiva da parte dei giovani.

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere in relazione a questa problematica.

Il fenomeno di "incitamento all'odio", negli ultimi anni si è fortemente diffuso e rafforzato soprattutto attraverso l'uso della Rete e i social network, dove si trovano forme di odio e hate speech online particolarmente violente. Per questo è importante affrontarlo con gli alunni/e anche a scuola. Il nostro Istituto intende intraprendere delle azioni in relazione a questa problematica attraverso l'educazione ad un uso etico e consapevole delle tecnologie e la promozione della consapevolezza di queste dinamiche in rete. Occorre, in tal senso, valorizzare la dimensione relazionale e fornire agli alunni 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. Inoltre, l'Istituto si potrà avvalere di esperti esterni per organizzare incontri formativi rivolti a docenti, genitori ed alunni (Polizia Postale, equipe Formazione Territoriale del MIUR, associazioni del Territorio preposte allo scopo...).

4.4 - Dipendenza da Internet e gioco online

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

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

La dipendenza da Internet, che può manifestarsi anche attraverso le ore trascorse online a giocare, rappresenta una questione importante per la comunità scolastica che deve attenzionare il fenomeno e fornire gli strumenti agli studenti e alle studentesse affinché questi siano consapevoli dei rischi che comporta l'iperconnessione. **La S.I.I.Pa.C**., la Società Italiana Intervento Patologie Compulsive, definisce la dipendenza da Internet come progressivo e totale assorbimento del soggetto alla Rete; di seguito alcune caratteristiche specifiche:

Dominanza. L'attività domina i pensieri ed il comportamento del soggetto, assumendo un

valore primario tra tutti gli interessi. **Alterazioni del tono dell'umore**. L'inizio dell'attività provoca cambiamenti nel tono dell'umore. Il soggetto prova un aumento d'eccitazione o maggiore rilassatezza come diretta conseguenza dell'incontro con l'oggetto della dipendenza. **Conflitto.** Conflitti inter-personali tra il soggetto e coloro che gli sono vicini, conflitti intrapersonali interni a se stesso, a causa del comportamento dipendente. **Ricaduta**. Tendenza a ricominciare l'attività dopo averla interrotta. I segnali patologici di questo che viene descritto come "un vero e proprio abuso della tecnologia", anche denominato "Internet Addiction Disorder" (I.A.D. coniato dallo psichiatra Ivan Goldberg 1996), sono specifici così come accade per le altre dipendenze più "tradizionali". In particolare, si hanno: la tolleranza ossia quando vi è un crescente bisogno di aumentare il tempo su internet e l'astinenza quando, cioè, vi è l'interruzione o la riduzione dell'uso della Rete che comporta ansia, agitazione psicomotoria, fantasie, pensieri ossessivi (malessere psichico e/o fisico che si manifesta quando s'interrompe o si riduce il comportamento). Tutto questo ha ripercussioni sulla sfera delle relazioni interpersonali che diventano via via più povere e alle quali si preferisce il mondo virtuale, con alterazioni dell'umore e della percezione del tempo.

Spesso il trascorrere del tempo online, in termini disfunzionali, è scandito dal gioco virtuale che può anche assumere forme di Dipendenza dal gioco online (Net gaming addiction o Internet Gaming Addiction). Le componenti che a livello bio-psico-sociale possono portare ad una vera e propria dipendenza sono sei. I sintomi sono:

- il giocatore è assorbito totalmente dal gioco;
- il giocatore è preoccupato e ossessionato dal gioco (si veda Lancini M., Il ritiro sociale negli adolescenti, Raffaello Cortina Ed., Milano, 2019);
- il gioco consente alla persona di sfuggire alla realtà con la sperimentazione di emozioni più piacevoli;
- il giocatore manifesta sempre di più l'impulso di giocare e di sperimentare emozioni positive;
- il giocatore sente di dover dedicare più tempo ai giochi;
- il giocatore se non può giocare manifesta ansia, depressione e irritabilità;
- può emergere un ritiro sociale;
- il giocatore, anche se comprende la gravità della situazione e sospende di giocare comunque non riesce a interrompere del tutto;
- il giocatore mente agli altri sull'utilizzo che fa dei giochi on line;
- il giocatore ha perso o mette a rischio relazioni o opportunità a causa dei giochi su Internet o ha perso interesse verso attività nella vita reale.

Anche in questo caso, la scuola ha la possibilità di fare formazione e di indicare strategie per un uso più consapevole delle tecnologie per favorire il "benessere digitale", cioè la capacità di creare e mantenere una relazione sana con la tecnologia.
La tecnologia infatti ha modificato gli ambienti che viviamo e ha un impatto sulla qualità della vita. Gli elementi che contribuiscono al benessere digitale sono:

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

Se controlliamo la tecnologia possiamo usarne il pieno potenziale e trarne dei vantaggi. La scuola può insegnare molto da questo punto di vista se integra la tecnologia nella didattica, mostrando un suo utilizzo funzionale che possa rendere più consapevoli gli alunni e le alunne delle proprie abitudini online. Si potrebbero strutturare regole condivise e stipulare con loro una sorta di "patto" d'aula e, infine, proporre delle alternative metodologiche e didattiche valide che abbiano come strumento giochi virtuali d'aula (adoperando la LIM o il dispositivo personale). È importante, quindi, non demonizzare la tecnologia o il gioco, ma cercare di entrare nel mondo degli/lle alunni/e, stabilendo chiare e semplici regole di utilizzo dei nuovi media.

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.

Il "sexting" è fra i rischi più diffusi connessi ad un uso poco consapevole della Rete. Il termine indica un fenomeno molto frequente che si verifica tra i giovanissimi che consiste nell'invio e/o la ricezione di contenuti mediali sessualmente espliciti che ritraggono se stessi o gli altri. Spesso i ragazzi e le ragazze lo fanno senza essere realmente consapevoli di scambiare materiale (pedopornografico) che potrebbe arrivare in mani sbagliate e avere conseguenze per i protagonisti delle immagini, delle foto e dei video. "Spesso sono realizzate con il telefonino, e vengono diffuse attraverso il cellulare (tramite invio di mms o condivisione tramite bluetooth) o attraverso siti, e-mail, chat. Spesso tali immagini o video, anche se inviate ad una stretta cerchia di persone, si diffondono in modo incontrollabile e possono creare seri problemi, sia personali che legali, alla persona ritratta.

Questi contenuti, infatti, 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 Si veda l'articolo 612 ter del codice penale rubricato "Diffusione illecita di immagini o video sessualmente espliciti").

Tra le caratteristiche del fenomeno vi sono principalmente:

- la fiducia tradita: chi produce e invia contenuti sessualmente espliciti ripone fiducia nel destinatario, credendo, inoltre, alla motivazione della richiesta (es. prova d'amore richiesta all'interno di una relazione sentimentale);
- la pervasività con cui si diffondono i contenuti: in pochi istanti e attraverso una condivisione

che diventa virale, il contenuto a connotazione sessuale esplicita può essere diffuso a un numero esponenziale e infinito di persone e ad altrettante piattaforme differenti. Il contenuto, così, diventa facilmente modificabile, scaricabile e condivisibile e la sua trasmissione è incontrollabile;

- la persistenza del fenomeno: il materiale pubblicato online può permanervi per un tempo illimitato e potrebbe non essere mai definitivamente rimosso. Un contenuto ricevuto, infatti, può essere salvato, a sua volta re-inoltrato oppure condiviso su piattaforme diverse da quelle originarie e/o in epoche successive.

La consapevolezza, o comunque la sola idea di diffusione di contenuti personali, si replica nel tempo e può finire con il danneggiare, sia in termini psicologici che sociali, sia il ragazzo/la ragazza soggetto della foto/del video che colui/coloro che hanno contribuito a diffonderla. Due agiti, quindi, che sono fra loro strettamente legati e che rappresentano veri e propri comportamenti criminali i quali hanno ripercussioni negative sulla vittima in termini di autostima, di credibilità, di reputazione sociale off e on line. A ciò si associano altri comportamenti a rischio, di tipo sessuale ma anche riferibili ad abuso di sostanze o di alcool. I rischi del sexting, legati al revenge porn, possono contemplare: violenza psicosessuale, umiliazione, bullismo, cyberbullismo, molestie, stress emotivo che si riversa anche sul corpo insieme ad ansia diffusa, sfiducia nell'altro/i e depressione. Per prevenire, quindi, il verificarsi di episodi di sexting, la scuola intraprenderà percorsi di informazione verso i genitori, proponendo l'utilizzo di forme di controllo parentale della navigazione in rete, e sensibilizzando gli alunni con contenuti adeguati inseriti nel curricolo scolastico, nell'ambito della tecnologia e dell'educazione civica.

4.6 - Adescamento online

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

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

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

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

La problematica dell'adescamento online (come quella del sexting) si inquadra in uno scenario più ampio di scarsa educazione emotiva, sessuale e di assenza di competenza digitale. Per prevenire i casi di adescamento online è opportuno accompagnare ragazze e ragazzi in un percorso di educazione (anche digitale) all'affettività e alla sessualità. Ciò aiuterebbe a renderli più sicuri emotivamente e pronti ad affrontare eventuali situazioni a rischio, imparando innanzitutto a gestire le proprie emozioni, il rapporto con il proprio corpo e con gli altri.

È molto importante, inoltre, che ragazzi e ragazze sappiano a chi rivolgersi in caso di problemi, anche quando pensano di aver fatto un errore, si vergognano o si sentono in colpa. Gli adulti coinvolti, genitori e docenti, devono essere un punto di riferimento per il minore che deve potersi fidare di loro e non sentirsi mai giudicato, ma compreso e ascoltato.
Fondamentale quindi, è portare avanti un percorso di educazione digitale che comprenda lo sviluppo anche di capacità quali la protezione della propria privacy e la gestione dell'immagine e dell'identità online, la capacità di gestire adeguatamente le proprie relazioni online (a partire dalla consapevolezza della peculiarità del mezzo/schermo che permette a chiunque di potersi presentare in modo da come è realmente). 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…). Per consigli e per un supporto è possibile rivolgersi agli operatori della Helpline di Generazioni Connesse (19696) che sono sempre a disposizione degli insegnanti, del Dirigente e degli operatori scolastici, oltre che dei bambini, degli adolescenti, dei genitori e di altri adulti per gestire nel modo più opportuno eventuali esperienze negative e/o problematiche inerenti l'utilizzo dei nuovi media.

4.7 - Pedopornografia

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

La legge n. 269 del 3 agosto 1998 *"Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di schiavitù", introduce nuove fattispecie di reato (come ad esempio il turismo sessuale) e, insieme alle successive modifiche e integrazioni contenute nella* ***legge n. 38 del 6 febbraio 2006*** *"Disposizioni in materia di lotta*

contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet", segna una tappa fondamentale nella definizione e predisposizione di strumenti utili a contrastare i fenomeni di sfruttamento sessuale a danno di minori. Quest'ultima, introduce, tra le altre cose, il reato di "pornografia minorile virtuale" (artt. 600 ter e 600 quater c.p.) che si verifica quando il materiale pedopornografico rappresenta immagini relative a bambini/e ed adolescenti, realizzate con tecniche di elaborazione grafica non associate, in tutto o in parte, a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali.

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

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

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

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

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

Il fenomeno dei sexting richiede di porre l'attenzione sulla necessità della prevenzione: i più giovani devono acquisire quelle competenze in grado di orientarli e guidarli nelle loro scelte anche online; per questo motivo, come già sottolineato, l'educazione, compresa l'educazione all'affettività, riveste un ruolo fondamentale. 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. Ad esempio, non è utile diffondere tra i bambini e le bambine più piccoli/e l'uso di servizi come le hotline, sia perché in caso di visione accidentale di materiale pedopornografico è opportuno che bambini/e possano parlarne con gli adulti di riferimento per la migliore risposta possibile, sia perché si potrebbe incentivare la ricerca proattiva, che comunque è vietata dalla legge italiana, per minori e per adulti. Risulta utilissima l'attività educativa sull'affettività e le relazioni, sottolineando sempre la necessità di rivolgersi ad un adulto quando qualcosa online mette a disagio. Pertanto, è auspicabile che a scuola ci sia un'attività di sensibilizzazione rivolta ai genitori e al personale scolastico, approfondendo la tematica facendo riferimento al Vademecum di Generazioni Connesse.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2019/2020).

Scegliere almeno 1 di queste azioni:

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

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

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

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

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

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

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

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

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

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

Scegliere almeno 1 di queste azioni:

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

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

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

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

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

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

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

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

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

Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

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

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

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

Nelle procedure:

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

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

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

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

Questo risulta importante sia per facilitare l'emersione di situazioni a rischio, e la conseguente presa in carico e gestione, sia per dare un messaggio chiaro a studenti e studentesse, alle famiglie e a tutti coloro che vivono la scuola che la stessa è un luogo sicuro, attento al benessere di chi lo vive, in cui le problematiche non vengono ignorate ma gestite con una mobilitazione attenta di tutta la comunità.

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

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

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

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

Vi suggeriamo, inoltre, i seguenti servizi:

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

- Clicca e segnala di Telefono Azzurro e STOP-IT di Save the Children Italia per segnalare la presenza di materiale pedopornografico online.

Segnalare eventuali problemi di cyberbullismo connessi a comportamenti di rischio online di alunni e alunne minorenni, rappresenta un'azione doverosa per il personale della scuola per tutelare i soggetti coinvolti. La segnalazione da parte dei docenti va fatta ogni qualvolta si ha il sospetto o la certezza che uno/a alunno/alunna possa essere vittima o responsabile

di una situazione di cyberbullismo, sexting o adescamento online. La segnalazione va fatta seguendo procedure condivise con l'intera comunità scolastica.

Le situazioni da segnalare sono quelle caratterizzate da ripetute aggressioni, finalizzate a insultare, diffamare, minacciare una persona tramite un utilizzo irresponsabile di Internet. In particolare si potranno segnalare:

- Contenuti afferenti la violazione della privacy (foto personali, l'indirizzo di casa o il telefono, password, informazioni private proprie o di amici, foto o video pubblicati contro la propria volontà, di eventi privati, ecc...).
- Contenuti afferenti all'aggressività o alla violenza (messaggi minacciosi, commenti offensivi, pettegolezzi, informazioni false, foto o video imbarazzanti, contenuti razzisti, che inneggiano al suicidio, immagini o video umilianti, virus, insulti, videogiochi pensati per un pubblico adulto, ecc...).
- Contenuti afferenti alla sessualità: messaggi molesti, conversazioni (testo o voce) che connotano una relazione intima e/o sessualizzata, foto o video personali con nudità o abbigliamento succinto, immagini pornografiche, foto e video in cui persone di minore età sono coinvolte o assistono ad attività sessuali (pedopornografia), ecc...
- Tutte le segnalazioni riportate dai docenti verranno registrate su apposita scheda.

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.

La segnalazione dei casi è un compito che deve coinvolgere l'intera comunità educante. Pertanto, per contrastare le situazioni problematiche, la scuola deve prevedere incontri di informazione e sensibilizzazione sui pericoli della Rete, suggerendo agli alunni di chiedere aiuto se pensano di vivere situazioni o di subire atti identificabili di bullismo o cyberbullismo. I docenti devono ascoltare gli alunni, osservando e monitorando il clima di classe, ciò che accade, le dinamiche relazionali nel contesto classe, senza fare indagini dirette; devono cercare, inoltre, di capire se gli episodi sono circoscritti al gruppo o se interessano l'intero Istituto. Sarebbe opportuno (sempre monitorando la situazione) prevedere momenti laboratoriali, utilizzando i contenuti e i materiali della piattaforma Generazioni Connesse, per stimolare il dialogo e la riflessione fra gli alunni e le alunne. L'insegnante che nota dei comportamenti anomali tra gli alunni della propria classe riconducibili a un disagio riferibile a un episodio di cyberbullismo, per la segnalazione dei casi, può utilizzare i seguenti strumenti, utili per raccogliere informazioni:

- Diario di Bordo o schema riepilogativo per la segnalazione dei rischi online (vedi allegato).
- Il modulo per la segnalazione dei casi (vedi allegato).

La segnalazione deve essere supportata da prove specifiche e/o testimonianze. Pertanto è necessario che l'Animatore Digitale e il docente conservi le prove della condotta incauta, scorretta o dell'abuso rilevate sui PC della scuola: soprattutto la data e l'ora, l'ID del mittente, il contenuto dei messaggi o l'indirizzo web del profilo e il suo contenuto. Per gli eventuali collegamenti non autorizzati a siti, social network, video-hosting sites e altri website, l'insegnante può conservare il link, stampare la pagina o salvare la schermata su documento Word. Per l'e-mail si può stampare la stessa o conservare l'intero messaggio, compresa l'intestazione del mittente. Nel caso di messaggi, si cercherà di risalire al mittente attraverso i dati del suo profilo. Sia nel caso di chat che di messaggi di posta elettronica, l'insegnante dovrà copiare e stampare i messaggi per fornire le

eventuali prove dell'indagine sugli abusi commessi. Conservare la prova è utile per far conoscere l'accaduto, in base alla gravità, ai genitori degli alunni, al Dirigente Scolastico e alla Polizia Postale. Qualora siano coinvolti più alunni, in qualità di vittime o di responsabili della condotta scorretta, le famiglie degli alunni in questione saranno informate tempestivamente per un confronto. La gestione dei casi rilevati andrà differenziata a seconda della loro gravità; in ogni caso è opportuno:

- annotare il comportamento sul registro;
- coinvolgere il referente d'Istituto per il contrasto del bullismo e del cyberbullismo valutando insieme le possibili strategie d'intervento;
- convocare i genitori (o chi esercita la responsabilità genitoriale) degli/delle alunni/alunne e colloquio con i docenti per condividere informazioni e strategie;
- richiedere la consulenza dello psicologo scolastico a supporto della gestione della situazione, in base alla gravità dell'accaduto;
- avvisare l'intero Consiglio di classe;
- informare il Dirigente Scolastico tramite relazione scritta. In base all'urgenza le comunicazioni formali possono essere precedute da quelle informali, effettuate per le vie brevi.

Nel caso di reati più gravi, sulla base della legge del 29 maggio, 71/2017, gli operatori scolastici hanno l'obbligo di effettuare la denuncia all'autorità giudiziaria (o alla Polizia Postale). Inoltre ci si potrà avvalere dei due servizi messi a disposizione dal Safer Internet Center il **"Clicca e Segnala"** di Telefono Azzurro e **"STOP-IT"** di Save the Children e del servizio Helpline del progetto Generazioni Connesse.

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.

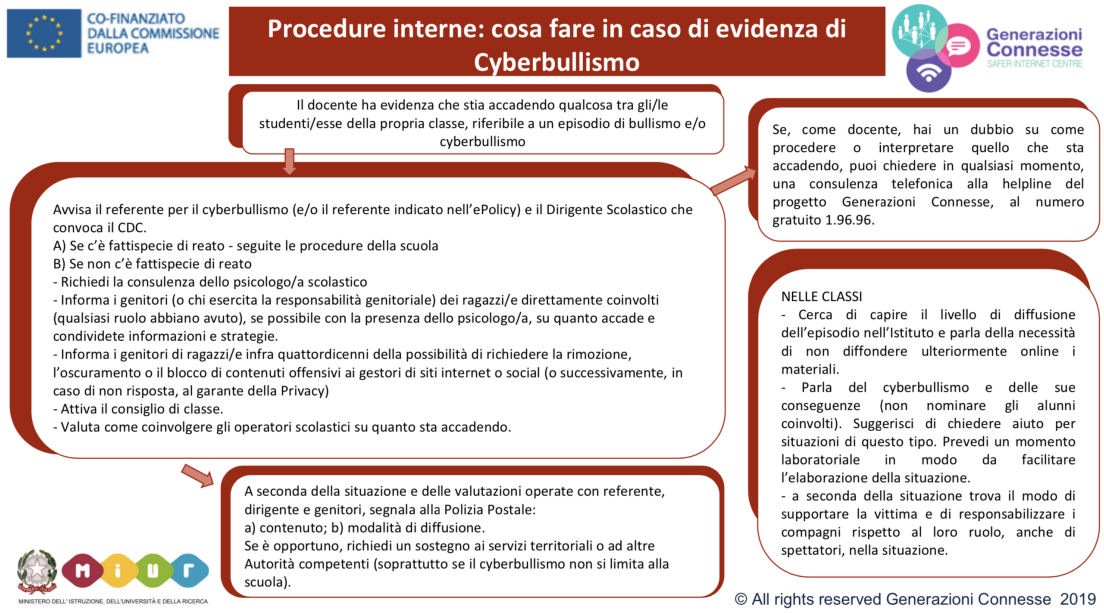
A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all'utilizzo di Internet può presentare.

- **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.

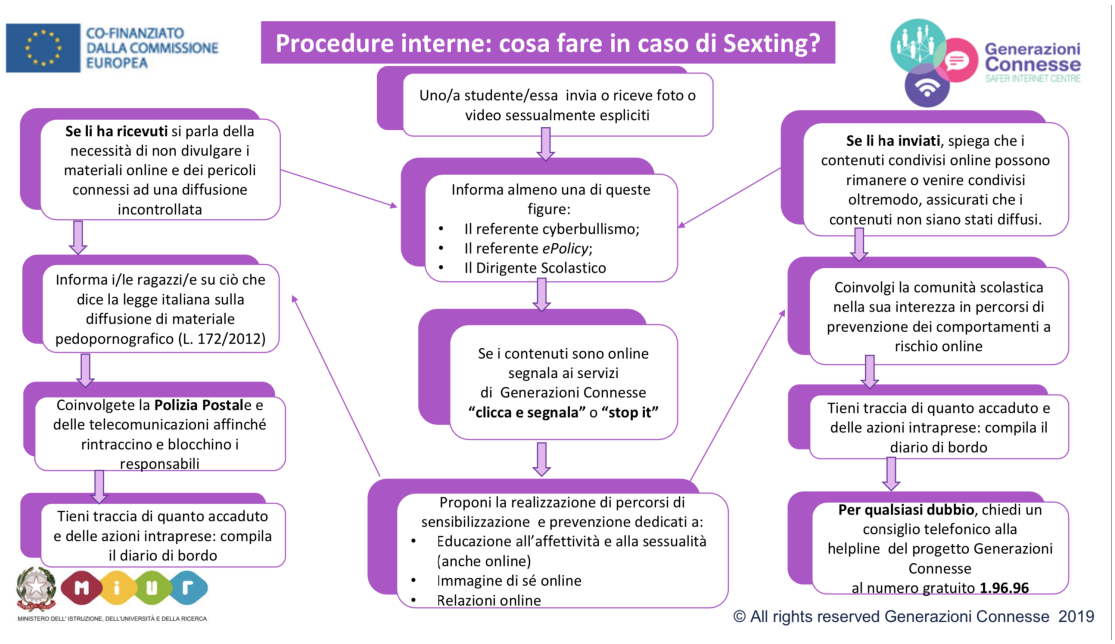
Nei casi di maggiore gravità, si coinvolgeranno gli attori esterni quali Forze dell'ordine, Servizi sociali, le ASL, etc… La relazione tra Scuola, Enti e Associazioni territoriali è molto importante in quanto il rapporto tra "comunità scolastica e territorio" contribuisce ad arricchire l'offerta formativa delle scuole. Tale rapporto deve essere improntato sempre con chiarezza e trasparenza, con precise informazioni all'utenza e a tutti coloro che sono coinvolti nelle tematiche affrontate. Sulla base delle segnalazioni/informazioni acquisite dalla scuola (su un caso di bullismo/cyberbullismo) si delinea il livello di priorità dell'intervento, da un livello meno grave a un livello sistematico più grave fino ad un livello molto grave di emergenza. In base, dunque, al livello di sofferenza psicologica delle singole persone coinvolte verranno delineate le azioni e gli interventi da intraprendere, decise dal Dirigente Scolastico, dal Consiglio di classe, dal referente del Bullismo e del Cyberbullismo della scuola e dalla famiglia, con la collaborazione dei Servizi Territoriali.

5.4. - Allegati con le procedure

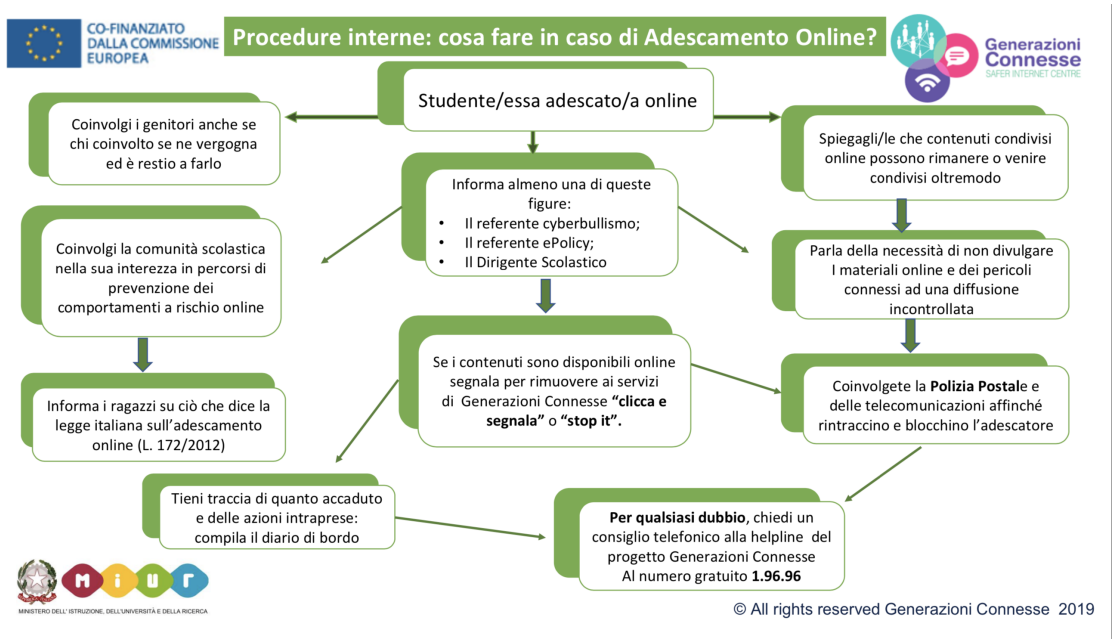
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



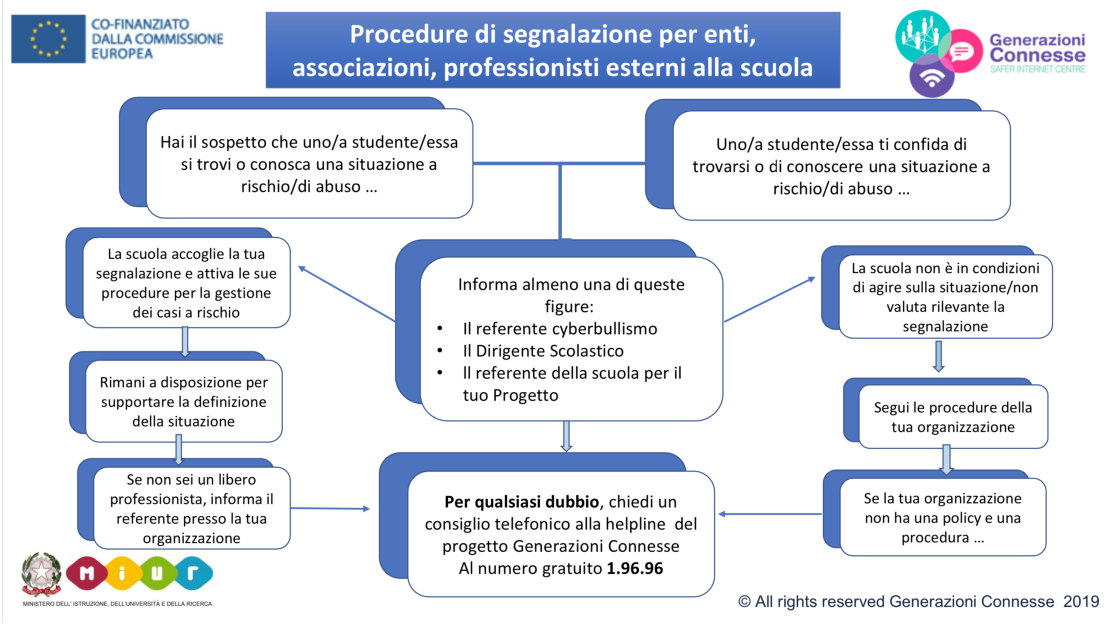
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



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



Altri allegati

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

Il nostro piano d'azioni

Non è prevista nessuna azione.