Istituto Statale di Istruzione Superiore
"LEONARDO DA VINCI"
I.T.E. "G. Agnelli" 0547-673576 - Liceo "E. Ferrari" 0547-675277
fois00400d@istruzione.it - fois00400d@pec.istruzione.it - www.isiscesenatico.edu.it
Dirigenza e Segreteria Viale dei Mille n° 158 – 47042 Cesenatico (FC) - 0547-675277
C. F. 90028640408 - FOIS00400D

E-POLICY DELL'I.S.I.S. "LEONARDO DA VINCI"
(Del. Consiglio di Istituto n. 39/2021 del 18 ottobre 2021)

Capitolo - 1.1 - Scopo dell'ePolicy

Le TIC (Tecnologie dell'informazione e della comunicazione) rappresentano strumenti fondamentali nel processo educativo e per l'apprendimento degli studenti e delle studentesse.
Le "competenze digitali" sono fra le abilità chiave all'interno del Quadro di riferimento Europeo delle Competenze per l'apprendimento permanente e di esse bisogna dotarsi proprio a partire dalla scuola (Raccomandazione del Consiglio Europeo del 2006 aggiornata al 22 maggio 2018, relativa alle competenze chiave per l'apprendimento permanente).
In un contesto sempre più complesso, diventa quindi essenziale per ogni Istituto Scolastico dotarsi di una E-policy, un documento programmatico volto a promuovere le competenze digitali ed un uso delle tecnologie positivo, critico e consapevole, sia da parte dei ragazzi e delle ragazze che degli adulti coinvolti nel processo educativo. L'E-policy, inoltre, vuole essere un documento finalizzato a prevenire situazioni problematiche e a riconoscere, gestire, segnalare e monitorare episodi legati ad un utilizzo scorretto degli strumenti.
L'E-policy ha l'obiettivo di esprimere la nostra visione educativa e proposta formativa, in riferimento alle tecnologie digitali. Nello specifico:

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

Argomenti del Documento

1. Presentazione dell'ePolicy
    1. Scopo dell'ePolicy
    2. Ruoli e responsabilità
    3. Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto
    4. Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica
    5. Gestione delle infrazioni alla ePolicy
    6. Integrazione dell'ePolicy con regolamenti esistenti

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

Perché è importante dotarsi di una E-policy?
Attraverso l'E-policy il nostro Istituto si vuole dotare di uno strumento operativo a cui tutta la comunità educante dovrà fare riferimento, al fine di assicurare un approccio alla tecnologia che sia consapevole, critico ed efficace, e al fine di sviluppare, attraverso specifiche azioni, una conoscenza delle opportunità e dei rischi connessi all'uso di Internet.
L' E-policy fornisce, quindi, delle linee guida per garantire il benessere in Rete, definendo regole di utilizzo delle TIC a scuola e ponendo le basi per azioni formative e educative su e con le tecnologie digitali, oltre che di sensibilizzazione su un uso consapevole delle stesse.

1.1 - Scopo dell'e-Policy

A fronte del varo del Piano Nazionale della Scuola Digitale e del recente lock-down che ha reso capillare l'uso delle TIC da parte di tutta la comunità educante (docenti, personale scolastico, studenti e famiglie), il nostro Istituto ha il compito di potenziare, nel corso degli anni, la propria dotazione tecnologica arredando tutte le classi con computer portatili o monitor fissi e Lim o schermi interattivi che permettono la realizzazione di attività didattiche su piattaforme educative telematiche. L'Istituto ha, inoltre, la necessità di porre particolare attenzione alla formazione del personale attivando o promuovendo corsi per l'acquisizione di competenze digitali, l'integrazione dell TIC nella didattica, l'utilizzo della piattaforma educativa Google Workspace. Infine, la scuola ha il dovere di creare e mantenere un ambiente sano e propositivo, per facilitare la crescita e lo studio personale di ciascun studente; ha l'obbligo, insieme alle famiglie, di responsabilizzare gli studenti alle relazioni tra pari, a promuovere il benessere di ciascuno e della collettività nell'ottica di una cittadinanza attiva.

Per questi motivi, diventa quindi prioritario l'elaborazione di un efficace strumento di e-policy con gli obiettivi di regolamentare l'utilizzo delle tecnologie digitali affinchè gli studenti e le studentesse ne dispongano in maniera positiva, critica e consapevole e di formare i docenti, i discenti e la comunità educanda tutta per accrescere e consolidare le competenze di cittadinanza digitale oltre ad un uso sicuro e creativo della rete e delle sue risorse. E', infine, necessario chiarire una serie di politiche preventive e di sensibilizzazione per contrastare comportamenti on-line a rischio.

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

1.2 - Ruoli e responsabilità

Il Dirigente Scolastico

Nel promuovere l'uso consentito delle tecnologie e di Internet, il ruolo del Dirigente Scolastico è quello di:

- garantire la tutela degli aspetti legati alla privacy e la tutela delle immagini di tutti i membri della comunità scolastica;
- garantire una formazione di base e specifica per tutte le figure scolastiche sulle Tecnologie di Informazione e della Comunicazione (ICT) che consenta loro di possedere le competenze necessarie all'utilizzo responsabile e consapevole di tali risorse;
- garantire l'esistenza di un sistema che consenta il monitoraggio e il controllo interno della sicurezza online di tutti i membri della comunità scolastica;
- regolare il comportamento degli studenti ed imporre sanzioni disciplinari in caso di comportamento inadeguato e uso improprio, in relazione all'utilizzo delle tecnologie digitali;
- dover informare tempestivamente, qualora venga a conoscenza di atti di cyberbullismo, che non si configurino come reato, i genitori dei minori coinvolti (o chi ne esercita la responsabilità genitoriale o i tutori).

Il Referente bullismo e cyberbullismo

Il ruolo del Referente per Bullismo e Cyberbullismo include i seguenti compiti:

- coordinare iniziative di prevenzione e 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;
- svolgere un importante compito di supporto al Dirigente, nonché all'Istituzione scolastica, per la revisione/stesura di Regolamenti, atti e documenti (PTOF, PdM, RAV, modello di e-policy d'Istituto);
- promuovere la conoscenza e la consapevolezza riguardo a bullismo e cyberbullismo, attraverso progetti d'Istituto che coinvolgano genitori, studenti e personale scolastico;
- collaborare in team con altre figure scolastiche (Animatore Digitale; Referente BES/Inclusione; Referente per la Dispersione);
- segnalare tempestivamente situazioni di rischio online o casi di bullismo o cyberbullismo;
- suggerire, incentivare e supportare progetti di Istituto relativi allo sviluppo nei discenti delle Competenze di Cittadinanza e Costituzione, nonché progetti di prevenzione ed informazione/formazione dell'intera comunità scolastica;
- coinvolgere gli altri soggetti della comunità scolastica, con particolare attenzione agli studenti/ex studenti (PEER EDUCATION);
- attivare uno SPORTELLO anonimo di segnalazione.

L'Animatore digitale e team dell'Innovazione

Il ruolo dell'Animatore Digitale, coadiuvato dal Team per l'Innovazione, include i seguenti compiti:

- stimolare la formazione interna all'istituzione negli ambiti di sviluppo della "scuola digitale" e fornire consulenza ed informazioni al personale in relazione ai rischi online e alle misure di prevenzione e gestione degli stessi;
- monitorare e rilevare le problematiche emergenti relative all'utilizzo sicuro delle TIC e di internet a scuola, nonché approntarsi all'individuazione di soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola;
- assicurare che gli utenti possano accedere alla rete della scuola solo tramite passwords applicate e regolarmente cambiate;
- coinvolgere l'intera comunità scolastica (alunni, genitori ed altri attori del territorio) nella partecipazione ad attività e progetti attinenti la "scuola digitale".

Tecnico informatico

Il ruolo del tecnico informatico si compone dei seguenti compiti:

- installare nuovi software;
- limitare attraverso un proxy l'accesso ad alcuni siti;
- controllare e coordinare, con l'ausilio di un opportuno registro, la prenotazione dei laboratori, consentendo in tal modo di tenere traccia di orari, laboratori e supporti utilizzati da ciascuno.

I Docenti

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

- provvedere personalmente alla propria formazione/aggiornamento sull'utilizzo del digitale con particolare riferimento alla dimensione etica (tutela della privacy, rispetto dei diritti intellettuali dei materiali reperiti in Internet e dell'immagine degli altri: lotta al cyberbullismo);
- supportare gli alunni nell'utilizzo consapevole delle tecnologie informatiche utilizzate a scopi didattici ed informarli/formarli sul divieto di plagio e sul rispetto della normativa vigente in merito ai diritti d'autore;
- segnalare al Dirigente scolastico e ai suoi collaboratori eventuali episodi di violazione delle norme di comportamento stabilite dalla scuola, avviando le procedure previste in caso di violazioni;
- supportare e indirizzare alunni coinvolti in problematiche legate alla rete.

Il personale Amministrativo, Tecnico e Ausiliario (ATA)

Il personale è tenuto ad assicurarsi di:

- avere adeguata consapevolezza riguardo alle questioni di sicurezza informatica, alla politica d'Istituto e relative buone pratiche;
- aver letto, compreso ed accettato il presente documento di E-Safety Policy;
- segnalare qualsiasi abuso, anche solo sospetto, al Dirigente Scolastico e/o all'Animatore Digitale per le opportune indagini/azioni/sanzioni;
- mantenere tutte le comunicazioni digitali con alunni e genitori/tutori a livello professionale e realizzandole esclusivamente attraverso canali ufficiali scolastici.

Gli Studenti e le Studentesse

Il ruolo degli studenti e delle studentesse prevede i seguenti compiti:

- leggere, comprendere ed accettare il documento di E-Safety Policy;
- comprendere e rispettare le norme sul diritto d'autore;

- avere consapevolezza delle situazioni di rischio legate alla rete, telefoni cellulari, fotocamere digitali;
- conoscere la politica della scuola sull'uso di dispositivi mobili e sull'uso delle immagini;
- comprendere l'importanza di adottare buone pratiche di sicurezza online quando si usano le tecnologie;
- adottare condotte rispettose degli altri anche durante la comunicazione in rete;
- comprendere l'importanza della segnalazione di ogni abuso, uso improprio, o accesso a materiali inappropriati, e conoscere il protocollo per tali segnalazioni;
- essere consapevoli del significato e della gravità di atti di cyberbullismo, a tutela della propria ed altrui incolumità, al fine di evitare di perpetrare violazioni al Regolamento d'Istituto ed al Patto di Corresponsabilità o, nei casi più gravi, reati punibili da parte della Magistratura;
- assumersi la responsabilità di un eventuale utilizzo sbagliato delle tecnologie.

I Genitori

Genitori e tutori svolgono un ruolo cruciale nel garantire che i minori comprendano la necessità di utilizzare in modo sicuro, consapevole ed appropriato dispositivi digitali e mobili. Per tale scopo è necessario che essi:

- contribuiscano, in sinergia con il personale scolastico, alla sensibilizzazione dei propri figli sul tema della sicurezza in rete;
- incoraggino l'impiego delle ICT da parte degli alunni nello svolgimento dei compiti a casa, controllando che tale impiego avvenga nel rispetto delle norme di sicurezza;
- sostengano l'Istituzione scolastica nel promuovere le buone pratiche di e-safety e, dunque, seguano le linee guida sull'uso appropriato di immagini digitali e video registrati in occasione di eventi scolastici, anche al di fuori delle aule;
- consultino periodicamente le sezioni del sito web loro dedicate, con particolare riguardo ed attenzione alla consultazione del registro elettronico;
- agiscano in modo concorde con la scuola per la prevenzione dei rischi e l'attuazione delle procedure previste in caso di violazione delle regole stabilite;
- rispondano per gli episodi commessi dai figli minori a titolo di culpa in educando (articolo 2048 del Codice civile). Infatti, sono esonerati da responsabilità solo se dimostrano di non aver potuto impedire il fatto. Ma nei casi più gravi per i giudici l'inadeguatezza dell'educazione impartita ai figli emerge dagli stessi episodi di bullismo, che per le loro modalità esecutive dimostrano maturità ed educazione carenti.

Gli Enti educativi esterni e le associazioni

Gli enti educativi esterni e le associazioni, che entrano in relazione con l'istituzione scolastica, hanno il compito di:

- osservare le politiche interne sull'uso consapevole della Rete e delle TIC;
- attivare procedure e comportamenti sicuri per la protezione degli studenti e delle studentesse, durante le attività che vengono svolte all'interno della scuola o in cui sono impegnati gli stessi.

Per quanto non espressamente indicato sui ruoli e sulle responsabilità delle figure presenti all'interno dell'Istituzione scolastica, si rimanda: all'art. 21, comma 8, Legge 15 marzo 1997, n. 59; all'art. 25 della Legge 30 marzo 2001, n. 165; al CCNL in vigore; al D.P.R. 8 marzo 1999, n. 275; alla Legge 13 luglio 2015, n. 107; al Piano Nazionale Scuola Digitale; a quanto statuito in materia di culpa in vigilando, culpa in organizzando, culpa in educando.

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

Tutti gli attori che entrano in relazione educativa con gli studenti e le studentesse devono: mantenere sempre un elevato profilo personale e professionale, eliminando atteggiamenti inappropriati, essere guidati dal principio di interesse superiore del minore, ascoltare e prendere in seria considerazione le opinioni ed i desideri dei minori, soprattutto se preoccupati o allertati per qualcosa.
Sono vietati i comportamenti irrispettosi, offensivi o lesivi della privacy, dell'intimità e degli spazi personali degli studenti e delle studentesse oltre che quelli legati a tollerare o partecipare a comportamenti di minori che sono illegali, o abusivi o che mettano a rischio la loro sicurezza.
Tutti gli attori esterni sono tenuti a conoscere e rispettare le regole del nostro Istituto dove sono esplicitate le modalità di utilizzo dei propri dispositivi personali (smartphone, tablet, pc, etc.) e quelli in dotazione della scuola, evitando un uso improprio o comunque deontologicamente scorretto durante le attività con gli studenti e le studentesse. Esiste l'obbligo di rispettare la privacy, soprattutto dei soggetti minorenni, in termini di fotografie, immagini, video o scambio di contatti personali (numero, mail, chat, profili di social network).

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

Al fine di rendere l'ePolicy uno strumento efficace per la tutela degli studenti e delle studentesse, intesa in senso ampio, è importante garantire la condivisione del regolamento di Istituto e delle norme di comportamento sopra citate con le organizzazioni/associazioni extrascolastiche e gli esperti esterni chiamati, a vario titolo, alla realizzazione di progetti ed attività educative, sul breve e/o lungo periodo.
E' importante, inoltre, garantire che tutti i soggetti esterni siano sensibilizzati e resi consapevoli dei rischi online che possono correre gli studenti e le studentesse e dei comportamenti corretti che devono adottare a scuola. Tale documento chiarisce, infatti, il sistema di azioni e le procedure di segnalazione da seguire, valide anche per i professionisti e le organizzazioni esterne, finalizzate a rilevare e gestire le problematiche connesse ad un uso non consapevole delle tecnologie digitali. In coerenza con il percorso intrapreso e con le azioni che l'Istituto già pone in essere, la predisposizione di un'informativa sintetica sull'ePolicy comprensiva delle procedure di segnalazione, significa

- garantire un migliore rapporto fiduciario fra scuola e famiglia;
- consentire di distinguere i ruoli e le azioni da compiere e di attivare direttamente, a seconda della tipologia dei casi da segnalare, le autorità competenti collaborando con i servizi del territorio per la prevenzione e la gestione di quanto rilevato, in un'ottica di gestione condivisa degli interventi;
- tutelare non solo gli alunni e la scuola stessa, ma anche porre in essere nuove modalità per rilevare, limitare e contrastare possibili pericoli legati a condotte educative non professionali.

In questo modo, si facilita la presa in carico da parte della scuola, qualora si verificassero problematiche derivanti da un utilizzo non corretto delle tecnologie digitali o quando, nei casi più estremi, si sospettassero forme di maltrattamento/abuso sia nel reale che nel virtuale, sia di tipo fisico che psicologico a danno di minori. Tale documento, inoltre, permette di tutelare ragazzi e ragazze da comportamenti potenzialmente rischiosi messi in atto da soggetti esterni alla scuola e che si trovano ad operare all'interno dell'Istituto.
L'informativa viene condivisa e sottoscritta nella stipula di eventuali contratti con personale e associazioni esterne: le figure professionali e le organizzazioni coinvolte in progetti, laboratori e attività devono, in altri termini, prendere visione di tutti i documenti proposti dall'Istituto e sottoscriverli preliminarmente all'avvio dei programmi con gli studenti e le studentesse, in classe o fuori.

- 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.

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

Onde evitare che l'adozione del presente documento rappresenti un mero atto formale, l'Istituto si impegna ad intraprendere una serie di azioni ed iniziative per la messa in atto della Policy. Oltre alla condivisione con l'intera comunità scolastica attraverso la pubblicazione sul sito della scuola, si prevede:
per il corpo docente:

- discussione in ambito collegiale sui contenuti, sulle pratiche indicate e su come declinare nel curriculo le tematiche d'interesse della policy;
- confronto collegiale, a cadenza annuale, riguardo alla necessità di apportare eventuali modifiche e/o miglioramenti alla policy vigente;
- elaborazione di protocolli condivisi di intervento;

per la componente studentesca:

- discussione in classe con il coordinatore sulla policy, nei primi giorni di attività scolastica, con particolare riguardo al protocollo di accoglienza per le nuove classi prime;
- diffusione tra gli studenti di un estratto del documento relativo, in particolare, ai comportamenti da attuare in caso di bisogno;
- lettura, comprensione e sottoscrizione del patto di corresponsabilità;

per i genitori:

- organizzazione di incontri di sensibilizzazione sul tema della sicurezza informatica e di informazione circa i comportamenti da monitorare o stigmatizzare;
- lettura e comprensione del Regolamento d'Istituto e sottoscrizione del Patto di Corresponsabilità.

- 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.

- 1.5 - Gestione delle infrazioni alla ePolicy

Le potenziali infrazioni in cui è possibile che gli alunni incorrano utilizzando le TIC ed internet, messi a loro disposizione dalla scuola a fini puramente didattici, o utilizzando i dispositivi personali sono prevedibilmente le seguenti:

- uso improprio della rete per esprimere giudizi, infastidire o impedire a qualcuno di esprimersi liberamente o partecipare al dialogo didattico-educativo;
- l'invio incauto o non autorizzato di immagini, foto o dati sensibili; la condivisione di immagini non appropriate, violente, intime o troppo spinte;
- la comunicazione incauta e non autorizzata con sconosciuti o soggetti comunque estranei all'azione didattico-educativa;

- il collegamento a siti web non indicati e, dunque, non autorizzati dai docenti durante attività laboratoriali di qualsiasi genere.

Le eventuali infrazioni delle e-Policy vengono gestite dal Consiglio di Classe, secondo le modalità deliberate dal Collegio dei Docenti. I provvedimenti disciplinari da adottare nei confronti di alunni che abbiano commesso una o più infrazione alla e-policy devono avere finalità educativa e tendere al rafforzamento del senso di responsabilità e, a seconda dei diversi gradi di gravità e di eventuali violazioni, si procederà con:

- richiamo verbale;
- sanzioni estemporanee commisurate alla gravità della violazione commessa;
- nota informativa ai genitori o tutori mediante registro elettronico;
- convocazione dei genitori o tutori per un colloquio con gli insegnanti;
- convocazione dei genitori o tutori per un colloquio con il Dirigente scolastico.

Contestualmente sono previsti interventi di carattere educativo di rinforzo dei comportamenti corretti e riparativi di eventuali disagi causati; di ridefinizione delle regole sociali di convivenza, attraverso la partecipazione consapevole ed attiva degli alunni delle classi coinvolte; di prevenzione e gestione positiva dei conflitti; di moderazione dell'eccessiva competitività, promozione dei rapporti amicali e di reti di solidarietà, di promozione della conoscenza e gestione delle emozioni.

- 1.6 - Integrazione dell'ePolicy con Regolamenti esistenti

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

- 1.6 - Integrazione dell'ePolicy con Regolamenti esistenti

Si allegano il regolamento di Istituto e il Patto di Corresponsabilità aggiornati alla luce del documento e-Policy redatto.

- 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.

- 1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

Il monitoraggio dell'implementazione della Policy avverrà contestualmente alla revisione del PTOF, a cura del Dirigente scolastico, dell'Animatore digitale e dei collaboratori del Dirigente, a seguito di verifica atta a constatare l'insorgenza di nuove necessità e la revisione di tecnologie esistenti.

Piano di azioni (*)

Azioni da svolgere entro un'annualità scolastica:

- Diffondere il presente documento tra tutti gli attori della comunità scolastica

- 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.

- 2.1. Curricolo sulle competenze digitali per gli studenti

L'elaborazione del curricolo digitale parte da una riflessione sui vari significati attribuibili al termine "competenza digitale". Come già evidente nella definizione iniziale delle Raccomandazioni Europee, le competenze digitali 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: è importante far riflettere i più giovani sul potenziale delle tecnologie digitali come strumenti per la risoluzione di problemi della vita quotidiana, onde evitare automatismi che abbiano conseguenze incerte, attraverso un’adeguata comprensione della “grammatica” dello strumento.
- 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: la prima fa riferimento alla capacità di gestire in modo sicuro i propri dati personali e quelli altrui, e di usare le tecnologie digitali per scopi eticamente accettabili e nel rispetto degli altri. La seconda, invece, pone un po’ più l’accento sulle pratiche sociali e quindi sullo sviluppo di particolari abilità socio-comunicative e partecipative per maturare una maggiore consapevolezza sui nostri doveri nei riguardi di coloro con cui comunichiamo online.

Premesso ciò, il curricolo prende spunto dai seguenti documenti che costituiscono un framework comune per le competenze digitali e l’educazione ai media degli studenti e delle studentesse:
- Piano Scuola Digitale (PNSD), in particolar modo il paragrafo 4.2. su “Competenze e contenuti”.
- Sillabo sull’Educazione Civica Digitale.
- DigComp 2.1. “Il quadro di riferimento per le competenze digitali dei cittadini”.
- Raccomandazione del Consiglio europeo relativa alle competenze chiave per l’apprendimento permanente (C189/9, p. 9).

In particolare, i seguenti moduli sono organizzati utilizzando le aree di competenza individuate all'interno del DigComp 2.1.

Modulo 1: Alfabetizzazione su informazioni e dati

L’area s’inquadra nella dimensione “informazionale” o “cognitiva” delle competenze digitali. Essa è relativa alla capacità di cercare, selezionare, valutare e riprocessare le informazioni in Rete.

Competenze:
1. Navigare, ricercare e filtrare dati, informazioni e i contenuti digitali;
2. Valutare dati, informazioni e contenuti digitali
3. Gestire dati, informazioni e contenuti digitali
4. Saper riconoscere e sapersi difendere da contenuti dannosi e pericolosi in Rete (es. app, giochi online, siti non adatti ai minori, materiale pornografico e pedo-pornografico etc.).

Modulo 2: Comunicazione e collaborazione

Quest’area fa riferimento a quelle competenze volte a riconoscere le giuste ed appropriate modalità per comunicare e relazionarsi online.

Competenze:
1. Interagire con gli altri attraverso le tecnologie digitali
2. Condividere informazioni attraverso le tecnologie digitali
3. Esercitare la cittadinanza attraverso le tecnologie digitali

4. Collaborare attraverso le tecnologie digitali
5. Netiquette
6. Gestire l'identità digitale

Modulo 3: Creazione di contenuti digitali.

Quest'area fa riferimento alle capacità di "valutare le modalità più appropriate per modificare, affinare, migliorare e integrare nuovi contenuti e informazioni specifici per crearne di nuovi e originali".

Competenze:

1. Sviluppare contenuti digitali
2. Integrare e rielaborare contenuti digitali
3. Copyright e licenze
4. Programmazione

Modulo 4: Sicurezza

Quest'area è parte di una dimensione più generale definita come "benessere digitale" che include la necessità di salvaguardare i propri dati personali e rispettare le regole nel trattare i dati altrui.

Competenze:

1. Proteggere i dispositivi
2. Proteggere i dati personali e la privacy
3. Proteggere la salute e il benessere
4. Proteggere l'ambiente

Modulo 5: Risolvere problemi

Competenze:

1. Risolvere problemi tecnici
2. Individuare fabbisogni e risposte tecnologiche
3. Utilizzare in modo creativo le tecnologie digitali
4. Individuare i divari di competenze digitali

- 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.

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

Su tali premesse l'Istituto, attraverso il collegio dei docenti, favorirà la partecipazione del personale ad iniziative promosse sia direttamente dalla scuola (ad es. con l'aiuto dell'animatore digitale) dalle reti di scuole e dall'amministrazione, sia quelle liberamente scelte dai docenti (anche online), purché restino coerenti con il piano di formazione.

L'Istituto potenzierà le azioni che via via sono state realizzate nell'ultimo triennio: l'uso integrato della G-Suite for Education, corsi di aggiornamento specifici relativi all'utilizzo e all'integrazione delle TIC nella Didattica e implementerà ulteriori azioni miranti al raggiungimento delle competenze specifiche sopra indicate.

- 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.

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

L'animatore e il team Digitale, insieme con la FS dell'area Formazione, anche su indicazione dei dipartimenti e sulla base della rilevazione dei bisogni formativi dei docenti, promuoveranno e organizzeranno i seguenti interventi formativi mirati:

1. azioni di formazione strutturate dall'Animatore con il team digitale e la funzione strumentale per la Formazione, con l'ausilio di esperti, sui rischi della rete;
2. azioni di formazione strutturate dall'Animatore con il team digitale e la funzione strumentale per la Formazione, sull'utilizzo della piattaforma educativa *G-Workspace for Education*;
3. azioni di sensibilizzazione ed informazione, a mezzo Circolari, rivolte ai docenti tutti sulle attività intraprese a livello ministeriale (Miur, USR, USP), dagli Osservatori regionali sul bullismo, dalle scuole Polo anche da enti formatori accreditati e qualificati;

Tali azioni verranno inserite nel Piano Triennale dell'Offerta Formativa e nel Piano di Formazione.

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.

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

A tale scopo la scuola:

1. recepisce quanto riportato nelle Linee di indirizzo del Miur riguardanti "Partecipazione dei genitori e corresponsabilità educativa" e aggiorna il "Patto di Corresponsabilità" e il "Regolamento di istituto" per ciò che attiene ad un uso consapevole, responsabile e condiviso delle tecnologie digitali da parte dei genitori nelle comunicazioni con la scuola e con i docenti (ad es. e-mail, gruppi WhatsApp ecc.) e alle nuove regole per gli studenti e le studentesse;
2. darà massima diffusione alle azioni intraprese dall'Istituto e rivolte alla comunità tutta attraverso circolari apposite e avvisi sulla home page del sito web istituzionale;
3. renderà nota, a mezzo circolare indirizzata anche ai genitori, la pubblicazione del documento di e-policy sul sito web del Liceo, Sezione Regolamenti.

Piano di azioni (*)

AZIONI (da sviluppare nell'arco dell'anno scolastico)

- Coinvolgere una rappresentanza dei genitori per individuare i temi di maggiore interesse nell'ambito dell'educazione alla cittadinanza digitale.
- Organizzare incontri con esperti per i genitori sull'educazione alla cittadinanza digitale.

- 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.

- 3.1 - Protezione dei dati personali

L' istituzione scolastica può trattare solamente i dati personali necessari al perseguimento di specifiche finalità istituzionali oppure quelli espressamente previsti dalla normativa di settore tutelandone la segretezza come previsto dalle leggi vigenti. In ogni caso viene fornito all'interessato (studente, genitore, docente) un'adeguata informativa sulle caratteristiche e le modalità dell'utilizzo dei loro dati, indicandone i responsabili del trattamento. Ove previsto, l'informativa comprende uno specifico e libero consenso, mediante apposita modulistica, nella quale viene indicato chiaramente quali saranno le finalità da perseguire, senza che vengano richiesti dati eccedenti rispetto a quanto strettamente necessario.

Lo studente e/o la propria famiglia hanno il diritto di conoscere quali informazioni che li riguardano sono conservate presso la scuola, di rettificare o aggiornare il contenuto. Per esercitare questi diritti è possibile rivolgersi direttamente al "titolare del trattamento" (la scuola) anche tramite suoi incaricati "responsabili del trattamento".

- 3.2 - Accesso ad Internet

1. *L'accesso a Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale.*
2. *Ogni persona ha eguale diritto di accedere a Internet in condizioni di parità, con modalità tecnologicamente adeguate e aggiornate che rimuovano ogni ostacolo di ordine economico e sociale.*
3. *Il diritto fondamentale di accesso a Internet deve essere assicurato nei suoi presupposti sostanziali e non solo come possibilità di collegamento alla Rete.*
4. *L'accesso comprende la libertà di scelta per quanto riguarda dispositivi, sistemi operativi e applicazioni anche distribuite.*

5. *Le Istituzioni pubbliche garantiscono i necessari interventi per il superamento di ogni forma di divario digitale tra cui quelli determinati dal genere, dalle condizioni economiche oltre che da situazioni di vulnerabilità personale e disabilità.*

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

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

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

- 3.2 - Accesso ad Internet

Ai fini dell'accesso ad Internet, la scuola è dotata sia di un'infrastruttura fisica che di un'infrastruttura senza fili.

L'infrastruttura fisica raggiunge tutte le aule dell'Istituto con almeno una presa ethernet (in alcuni casi anche due) funzionale a garantire il collegamento Internet dei dispositivi presenti in classe.

La rete Wi-Fi consente l'accesso ad Internet mediante l'inserimento di credenziali personali, distribuite e gestite dal personale tecnico. La rete Wi-Fi prevede filtri e limitazioni tali da impedire la navigazione internet verso siti web o servizi inappropriati e potenzialmente dannosi.

- 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.

- 3.3 - Strumenti di comunicazione online

L'Istituto fa uso di strumenti di comunicazione online sia per la comunicazione interna, sia per quella esterna.

La comunicazione interna è realizzata attraverso gli strumenti di seguito elencati:

- il registro elettronico: è lo strumento privilegiato per quanto riguarda la comunicazione con le famiglie; esso consente di visionare l'andamento scolastico (assenze, argomenti lezioni e compiti, note disciplinari) e i risultati scolastici (voti, documenti di valutazione); è utilizzato dai genitori per prenotare colloqui individuali con i docenti e dalla scuola per diramare comunicazioni varie.
- e-mail istituzionale: tutto il personale scolastico (docenti e personale ATA), nonché tutti gli studenti, possiedono una casella di posta personale con dominio @davincicesenatico.it che viene utilizzata regolarmente per le comunicazioni interne fra i vari soggetti dell'istituzione scolastica.

La comunicazione esterna è realizzata sul sito istituzionale. Gli avvisi di maggiore importanza vengono sempre visualizzati sulla *home page*, che viene aggiornata regolarmente per garantire una pronta comunicazione con l'esterno; inoltre, il sito è dotato di molteplici sezioni dedicate ai vari servizi offerti dall'Istituto (orientamento, Albo Online, servizi di segreteria ecc.).

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.

- 3.4 - Strumentazione personale

Il nostro Istituto promuove l'uso dei dispositivi elettronici durante lo svolgimento dell'attività didattica, favorendo anche approcci di tipo BYOD. L'uso del proprio smartphone o del proprio tablet viene pertanto consentito purché lo stesso avvenga previa autorizzazione del docente e nel pieno rispetto degli altri utenti e componenti della classe. L'uso scorretto del dispositivo personale, qualora accertato dal docente direttamente o dietro segnalazione, sarà perseguito e sanzionato in accordo con quanto previsto dal Regolamento di Istituto.

Di seguito, i dieci i punti del Miur per l'uso dei dispositivi mobili a scuola, BYOD (Bring your own device):

1. Ogni novità comporta cambiamenti. Ogni cambiamento deve servire per migliorare l'apprendimento e il benessere delle studentesse e degli studenti e più in generale dell'intera comunità scolastica
2. I cambiamenti non vanno rifiutati, ma compresi e utilizzati per il raggiungimento dei propri scopi. Bisogna insegnare a usare bene e integrare nella didattica quotidiana i dispositivi, anche attraverso una loro regolamentazione. Proibire l'uso dei dispositivi a scuola non è la soluzione. A questo proposito ogni scuola adotta una Politica di Uso Accettabile (PUA) delle tecnologie digitali.
3. La scuola promuove le condizioni strutturali per l'uso delle tecnologie digitali. Fornisce, per quanto possibile, i necessari servizi e l'indispensabile connettività, favorendo un uso responsabile dei dispositivi personali (BYOD). Le tecnologie digitali sono uno dei modi per sostenere il rinnovamento della scuola.
4. La scuola accoglie e promuove lo sviluppo del digitale nella didattica. La presenza delle tecnologie digitali costituisce una sfida e un'opportunità per la didattica e per la cultura scolastica. Dirigenti e insegnanti attivi in questi campi sono il motore dell'innovazione. Occorre coinvolgere l'intera comunità scolastica anche attraverso la formazione e lo sviluppo professionale.
5. I dispositivi devono essere un mezzo, non un fine. È la didattica che guida l'uso competente e responsabile dei dispositivi. Non basta sviluppare le abilità tecniche, ma occorre sostenere lo sviluppo di una capacità critica e creativa.

6. L’uso dei dispositivi promuove l’autonomia delle studentesse e degli studenti. È in atto una graduale transizione verso situazioni di apprendimento che valorizzano lo spirito d’iniziativa e la responsabilità di studentesse e gli studenti. Bisogna sostenere un approccio consapevole al digitale nonché la capacità d’uso critico delle fonti di informazione, anche in vista di un apprendimento lungo tutto l’arco della vita.
7. Il digitale nella didattica è una scelta: sta ai docenti introdurla e condurla in classe. L’uso dei dispositivi in aula, siano essi analogici o digitali, è promosso dai docenti, nei modi e nei tempi che ritengono più opportuni.
8. Il digitale trasforma gli ambienti di apprendimento. Le possibilità di apprendere sono ampliate, sia per la frequentazione di ambienti digitali e condivisi, sia per l’accesso alle informazioni, e grazie alla connessione continua con la classe. Occorre regolamentare le modalità e i tempi dell’uso e del non uso, anche per imparare a riconoscere e a mantenere separate le dimensioni del privato e del pubblico.
9. Rafforzare la comunità scolastica e l’alleanza educativa con le famiglie. È necessario che l’alleanza educativa tra scuola e famiglia si estenda alle questioni relative all’uso dei dispositivi personali. Le tecnologie digitali devono essere funzionali a questa collaborazione. Lo scopo condiviso è promuovere la crescita di cittadini autonomi e responsabili.
10. Educare alla cittadinanza digitale è un dovere per la scuola. Formare i futuri cittadini della società della conoscenza significa educare alla partecipazione responsabile, all’uso critico delle tecnologie, alla consapevolezza e alla costruzione delle proprie competenze in un mondo sempre più connesso.

Anche il progetto Generazioni Connesse, d’altra parte, va verso la responsabilizzazione di tutti i soggetti in gioco nel processo educativo e didattico dove l’utilizzo delle tecnologie e dei dispositivi anche personali va mediato e calibrato sviluppando un pensiero critico. Laddove lo strumento viene utilizzato per integrare la didattica per attività in modalità BYOD, come previsto dal PNSD, si prevede che, con la condivisione della presente Policy, “le famiglie si assumono l’impegno di rispondere direttamente dell’operato dei propri figli nel caso in cui, ad esempio, gli stessi arrechino danni ad altre persone” a seguito di violazioni della presente policy”.

Piano di azioni (*)

AZIONI (da sviluppare nell’arco dell’anno scolastico)

Informare studenti ei genitori su indicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola

- 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.*

Testo personalizzato - 4.1 - Sensibilizzazione e Prevenzione

La sensibilizzazione costituisce il primo passo verso un cambiamento positivo, ma per far sì che l'intervento sia efficace, è importante che sia chiara l'azione verso cui i soggetti devono impegnarsi. Due sono gli aspetti che bisogna tenere in considerazione: la consapevolezza dello status quo e la motivazione al cambiamento. E' quindi importante fornire ai beneficiari informazioni chiare su quello che è lo stato attuale del tema che si vuole trattare. In questo modo gli utenti avranno tutte le informazioni necessarie per avere una fotografia chiara del contenuto che si sta trattando e del perché è necessario impegnarsi verso un cambiamento (motivazione al cambiamento). Il nostro Istituto, partendo dall'analisi della situazione attuale e dei bisogni reali, intende sviluppare una riflessione sul tema dei rischi on line e promuovere negli alunni, nei docenti e nelle famiglie la consapevolezza dei comportamenti pericolosi attraverso la diffusione di informazioni.

Per prevenzione si intende un insieme molto ampio di strategie che coinvolgono le famiglie e le forze sociali che operano sul

territorio al fine di mettere al proprio centro l'educazione formativa dei ragazzi. Nello specifico il nostro Istituto attiverà una serie di misure volte a prevenire e contrastare bullismo e cyberbullismo, promuovendo azioni di formazione per sviluppare le competenze digitali degli studenti e delle studentesse, nonchè dei docenti e del personale scolastico, al fine di un uso consapevole e sicuro delle TIC. Inoltre, si propone di supportare e implementare la competenza digitale di tutti i ragazzi all'interno delle materie curricolari.

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

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

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).

- 4.2 - Cyberbullismo: che cos'è e come prevenirlo

4.2.1. Le caratteristiche del fenomeno

Le caratteristiche tipiche del bullismo sono l'intenzionalità, la persistenza nel tempo, l'asimmetria di potere e la natura sociale del fenomeno (Olweus, 1996), ma nel cyberbullismo intervengono anche altri elementi, quali:

- L'impatto: la diffusione di materiale tramite Internet è incontrollabile e non è possibile prevederne i limiti. Un contenuto offensivo e denigratorio online può, quindi, diventare virale e distruggere in alcuni casi 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. È importante tenere bene a mente, però, che quello dell'anonimato è un "falso mito della Rete". Ogni nostra azione online è, infatti, rintracciabile e riconducibile a noi con gli strumenti opportuni o con l'intervento della Polizia Postale. L'anonimato del cyberbullo, inoltre, è anche uno dei fattori che stanno alla base del forte stress percepito dalla vittima, la quale molte volte non può dare né un nome e né un volto al proprio aggressore;
- Assenza di confini spaziali: il cyberbullismo può avvenire ovunque, invadendo anche gli spazi personali e privando l'individuo dei suoi spazi-rifugio. La vittima può essere raggiungibile anche a casa e vive nella costante percezione di non avere vie di fuga.
- Assenza di limiti temporali: può avvenire a ogni ora del giorno e della notte.
- Indebolimento dell'empatia: quando le interazioni avvengono prevalentemente online, la riduzione di empatia che ne consegue può degenerare nei comportamenti noti messi in atto dai cyberbulli.
- Feedback non tangibile: il cyberbullo non vede in modo diretto le reazioni della vittima e, ancora una volta, ciò riduce fortemente l'empatia e il riconoscimento del danno provocato. Per questo il cyberbullo non è mai totalmente consapevole delle conseguenze delle proprie azioni. L'impossibilità di vedere con i propri occhi l'eventuale sofferenza e umiliazione provata dalla vittima fa sì che il tutto venga percepito come "uno scherzo" divertente a cui partecipare, di cui ridere o a cui essere indifferenti. Inoltre, il cyberbullismo non lascia segni fisici evidenti sulla vittima e si consuma in un contesto virtuale che spesso viene percepito dai ragazzi come non "reale", come un mondo ludico a sé stante.

È molto importante sottolineare come il cyberbullismo non sia una problematica che riguarda unicamente vittima e

cyberbullo. È un fenomeno sociale e di gruppo. Infatti, centrale è il ruolo delle agenzie educative e di socializzazione (formali e informali) più importanti per gli adolescenti: la famiglia, la scuola, i media, le tecnologie digitali e il gruppo dei pari.

4.2.2. Riferimenti legislativi e responsabilità giuridica

Chi compie atti di bullismo e cyberbullismo può anche essere responsabile di reati penali e danni civili e imputabile se, nel momento del fatto, abbia compiuto quattordici anni. Secondo il codice penale italiano i comportamenti penalmente rilevanti in questi casi sono:

- Per il bullismo:

- percosse (art. 581 c.p.)
- lesioni (art. 582 c.p.)
- ingiuria (art. 594 c.p.depenalizzato D.lgs 7/2016)
- deturpamento di cose altrui (art. 639 c.p.)

- Per il cyberbullismo:

- diffamazione aggravata (art. 595/3 c.p.)
- violenza privata (art. 610 c.p.)
- trattamento illecito dei dati personali (art. 167 T.U. privacy)
- sostituzione di persona (art. 494 c.p.)
- accesso abusivo a un sistema informatico (art. 615 ter c.p.)
- estorsione sessuale (art. 629 c.p.)
- molestie e stalking (art. 660 c.p. e art. 612 bis c.p.)

Per quanto riguarda la responsabilità del minorenne, secondo il diritto civile, risponde:

- il genitore per culpa in educando e culpa in vigilando (art. 2048, I co, c.c.)
- la scuola per culpa in vigilando (art. 2048, II e III co, c.c.)

Si precisa che l'affidamento alla vigilanza di terzi solleva i genitori dalla presunzione di culpa in vigilando, ma non anche da quella di culpa in educando. Si precisa, inoltre, che il docente, in quanto pubblico ufficiale, è tenuto a denunciare alle autorità competenti qualunque illecito rechi danno al minore. I genitori sono pertanto responsabili dei figli minori sia per quanto concerne gli illeciti comportamenti che siano frutto di omessa o carente sorveglianza, sia per quanto concerne gli illeciti riconducibili ad oggettive carenze nell'attività educativa, che si manifestino nel mancato rispetto delle regole della civile coesistenza, vigenti nei diversi ambiti del contesto sociale in cui il soggetto si trovi ad operare.

4.2.3. Come intervenire?

La Legge 71/2017 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 prevede azioni preventive ed educative e non solo sanzionatorie. A tal fine, può avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio e 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). Si allega il "protocollo d'Istituto per la prevenzione e il contrasto del fenomeno del bullismo e del cyberbullismo" (Delibera del Consiglio di Istituto n.55 del 22 dicembre 2020).

- 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.

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

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

La prima azione suggerita riguarda incontri di sensibilizzazione con le classi al fine di aumentare la consapevolezza del fenomeno.

Tali incontri si focalizzeranno sullo smontaggio di alcune convinzioni che potrebbero risultare fuorvianti e percorsi di sensibilizzazione sulle competenze necessarie per vivere nella dimensione di iper-connessione.

Gli studenti, pertanto, saranno sollecitati a lavorare su se stessi attraverso:

- prestare attenzione ai post che si scrivono o che si ricondividono e alle affermazioni che si fanno poiché le parole in rete sono "nude" (non hanno l'ausilio del nostro corpo) e quindi maggiormente fraintendibili.
- esercitarsi ad entrare in relazione con gli altri. L'uso di video e le tecniche di role playing possono aiutare a modellare le forme della comunicazione quotidiana per evitare di alimentare scambi verbali ostili.
- esercitare il dubbio rispetto a ciò che si legge, spesso scritto appositamente per provocare una reazione istintiva;
- imparare a decodificare meglio il mondo che ci circonda e a parlarne in modo più riflesso.
- il tener presente che le parole scritte sono quasi immortali, pubbliche quindi incontrollabili, sia come numero di lettori sia come possibile passaggio da un canale all'altro e dall'online all'offline.

Il nostro Istituto si attiverà sulla formazione degli studenti attraverso il potenziamento delle loro abilità comunicative sulle quali si può fondare una successiva competenza sociale.

Il training ed il coinvolgimento di insegnanti nel progetto sulle competenze comunicative diventano importanti per la buona riuscita del progetto stesso. Gli insegnanti saranno introdotti alla conoscenza dei siti che in Rete propongono materiale didattico atto a diffondere consapevolezza sull'uso del linguaggio e che utilizzeranno all'interno delle proprie discipline.

- 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.

4.4 - Dipendenza da Internet e gioco online

Il nostro Istituto promuoverà, nell'ambito degli esistenti percorsi formativi, interventi sul benessere digitale, data la rilevante diffusione di tale fenomeno.

Infatti 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.

La scuola, anche in questo caso, 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 vantaggi. 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 (Es. adoperando la LIM o il dispositivo personale). È importante, quindi, non demonizzare la tecnologia o il gioco, ma cercare di entrare nel mondo degli/lle studenti/studentesse, stabilendo chiare e semplici regole di utilizzo.

- 4.5 - Sexting

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

- 4.5 - Sexting

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

- 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).

- 4.6 - Adescamento online

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

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…).

L'adescamento, inoltre, può essere una problematica molto delicata da gestire e può avere ripercussioni psicologiche significative sul minore. Per questo potrebbe essere necessario rivolgersi ad un Servizio territoriale (es. Consultorio Familiare, Servizio di Neuropsichiatria Infantile, ecc.) in grado di fornire alla vittima anche un adeguato supporto di tipo psicologico o psichiatrico. I minori vittime di adescamento riferiscono, generalmente, di sentirsi traditi, ma anche di provare un senso di colpa per essere caduti in trappola ed essersi fidati di uno sconosciuto. Inutile sottolineare che nei casi più estremi in cui l'adescamento porta ad un incontro fisico e ad un abuso sessuale un sostegno psicologico esperto per il minore è da considerarsi prioritario e urgente.

Per consigli e per un supporto è possibile rivolgersi alla Helpline di Generazioni Connesse (19696).

- 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.

- 4.7 - Pedopornografia

Risulta utilissima l'attività educativa sull'affettività e le relazioni, sottolineando sempre la necessità di rivolgersi ad un adulto quando qualcosa online mette a disagio. Parallelamente, se si ravvisa un rischio per il benessere psicofisico dei/lle bambini/e, ragazzi/e coinvolte nella visione di questi contenuti sarà opportuno ricorrere a un supporto psicologico anche passando per una consultazione presso il medico di base o pediatra di riferimento. Le strutture pubbliche a cui rivolgersi sono i servizi socio-sanitari del territorio di appartenenza: Consultori Familiari, Servizi di Neuropsichiatria infantile, centri specializzati sull'abuso e il maltrattamento all'infanzia, etc.
Se si è a conoscenza di tale tipologia di reato è possibile far riferimento alla: Polizia di Stato – Compartimento di Polizia postale e delle Comunicazioni; Polizia di Stato – Questura o Commissariato di P.S. del territorio di competenza; Arma dei Carabinieri – Comando Provinciale o Stazione del territorio di competenza; Polizia di Stato – Commissariato online.

Piano di azioni (*)

AZIONI (da sviluppare nell'arco dell'anno scolastico)
□ Diffusione di informazione sui rischi connessi a tutti gli attori della comunità scolastica

- 5.1. - Cosa segnalare

Il personale docente del nostro Istituto quando ha il sospetto o la certezza che uno/a studente/essa possa essere vittima o responsabile di una situazione di cyberbullismo, sexting o adescamento online ha a disposizione procedure definite e può fare riferimento a tutta la comunità scolastica.
Questa sezione dell'ePolicy contiene le procedure standardizzate per la segnalazione e gestione dei problemi connessi a comportamenti online a rischio di studenti e studentesse (vedi allegati a seguire). Tali procedure dovranno essere una guida costante per il personale della scuola nell'identificazione di una situazione online a rischio, così da definire le modalità di presa in carico da parte della scuola e l'intervento migliore da mettere in atto per aiutare studenti/esse in difficoltà. Esse, inoltre, forniscono valide indicazioni anche per i professionisti e le organizzazioni esterne che operano con la scuola (vedi paragrafo 1.3. dell'ePolicy).
Nelle procedure:

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

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

Nell'affrontare i casi prevediamo la collaborazione con altre figure, enti, istituzioni e servizi presenti sul territorio (che verranno richiamati più avanti), qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.
Tali procedure sono comunicate e condivise con l'intera comunità scolastica.
Questo risulta importante sia per facilitare l'emersione di situazioni a rischio, e la conseguente presa in carico e gestione, sia per dare un messaggio chiaro a studenti e studentesse, alle famiglie e a tutti coloro che vivono la scuola che la stessa è un luogo sicuro, attento al benessere di chi lo vive, in cui le problematiche non vengono ignorate ma gestite con una mobilitazione attenta di tutta la comunità.
La condivisione avverrà attraverso assemblee scolastiche che coinvolgono i genitori, gli studenti e le studentesse e il personale della scuola, con l'utilizzo di locandine da affiggere a scuola, attraverso news nel sito della scuola e durante i collegi docenti e attraverso tutti i canali maggiormente utili ad un'efficace comunicazione.
A seguire, le problematiche a cui fanno riferimento le procedure allegate:

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

Per quanto riguarda la necessità di segnalazione e rimozione di contenuti online lesivi, ciascun minore ultraquattordicenne (o i suoi genitori o chi esercita la responsabilità del minore) che sia stato vittima di cyberbullismo può inoltrare al titolare del trattamento o al gestore del sito internet o del social media un'istanza per l'oscuramento, la rimozione o il blocco dei contenuti diffusi nella Rete. Se entro 24 ore il gestore non avrà provveduto, l'interessato può rivolgere analoga richiesta al Garante per la protezione dei dati personali, che rimuoverà i contenuti entro 48 ore.
Vi suggeriamo, inoltre, i seguenti servizi:
- Servizio di Helpline 19696 e Chat di Telefono Azzurro per supporto ed emergenze;
- Clicca e segnala di Telefono Azzurro e STOP-IT di Save the Children Italia per segnalare la presenza di materiale pedopornografico online.

5.1. - Cosa segnalare

Tra i principali rischi segnaliamo:

- Possibile esposizione a contenuti violenti o uso di videogiochi diseducativi;

- Esposizione a siti violenti, razzisti, che invitano a comportamenti pericolosi per il benessere psicofisico della persona
- Possibili contatti con individui malintenzionati (adescamento/ grooming);
- Gioco d'azzardo online;
- Violazione della privacy o furto di identità in rete;
- Uso della comunicazione in rete offensivo e lesivo della dignità propria o altrui;
- Utilizzo di tecnologie informatiche e dispositivi mobili senza autorizzazione dei Docenti;
- Rischio di molestie o maltrattamenti da coetanei (bullismo e cyberbullismo);
- Scambio di materiale a sfondo sessuale (sexting e pedopornografia)

Le procedure indicate in questa sezione si riferiscono, oltre a quelle sopra indicate, legate ad un utilizzo scorretto delle TIC (Tecnologie dell'Informazione e della Comunicazione), anche a tutte le azioni da mettere in pratica per la presa in carico e relativa gestione delle situazioni di bullismo e cyberbullismo.

- 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.

5.2. - Come segnalare: quali strumenti e a chi

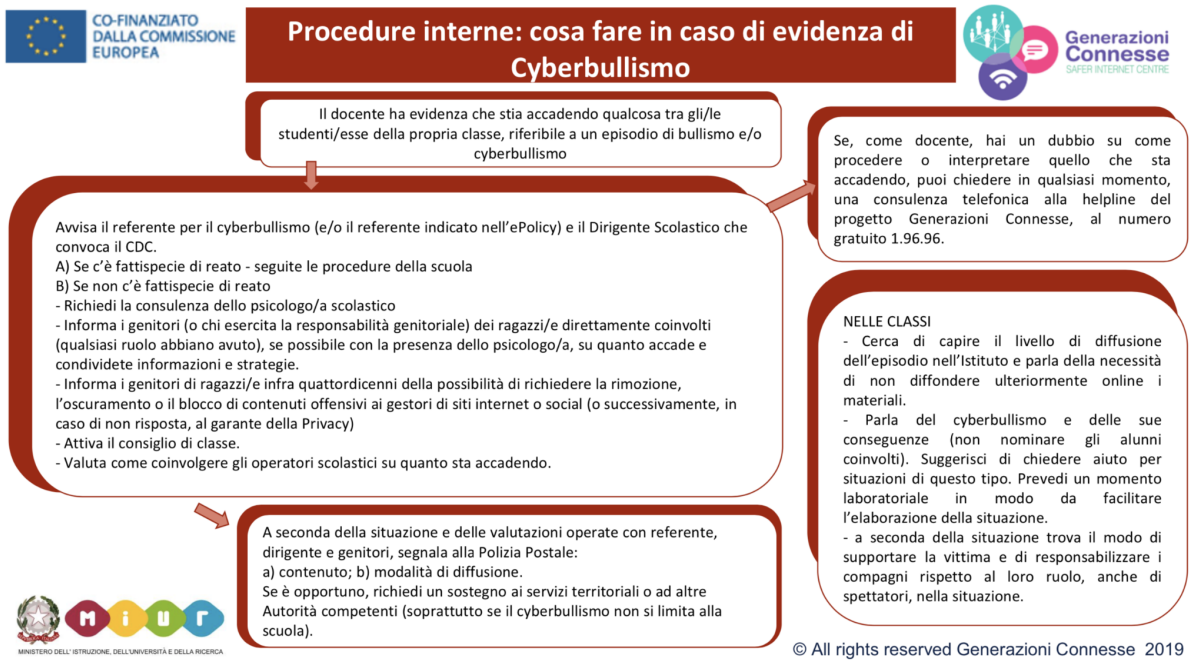
- 5.3. - Gli attori sul territorio

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.

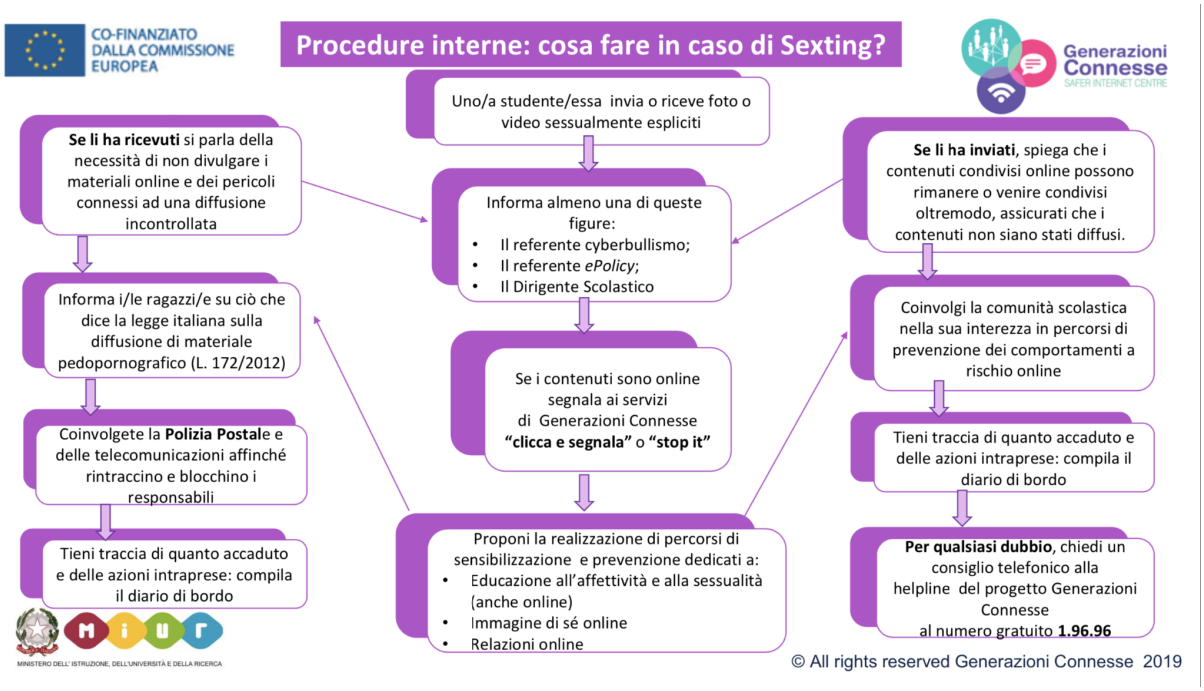
Per una mappatura degli indirizzi di tali strutture è possibile consultare il Vademecum di Generazioni Connesse “Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all’utilizzo delle tecnologie digitali da parte dei più giovani” (seconda parte, pag. 31), senza 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.

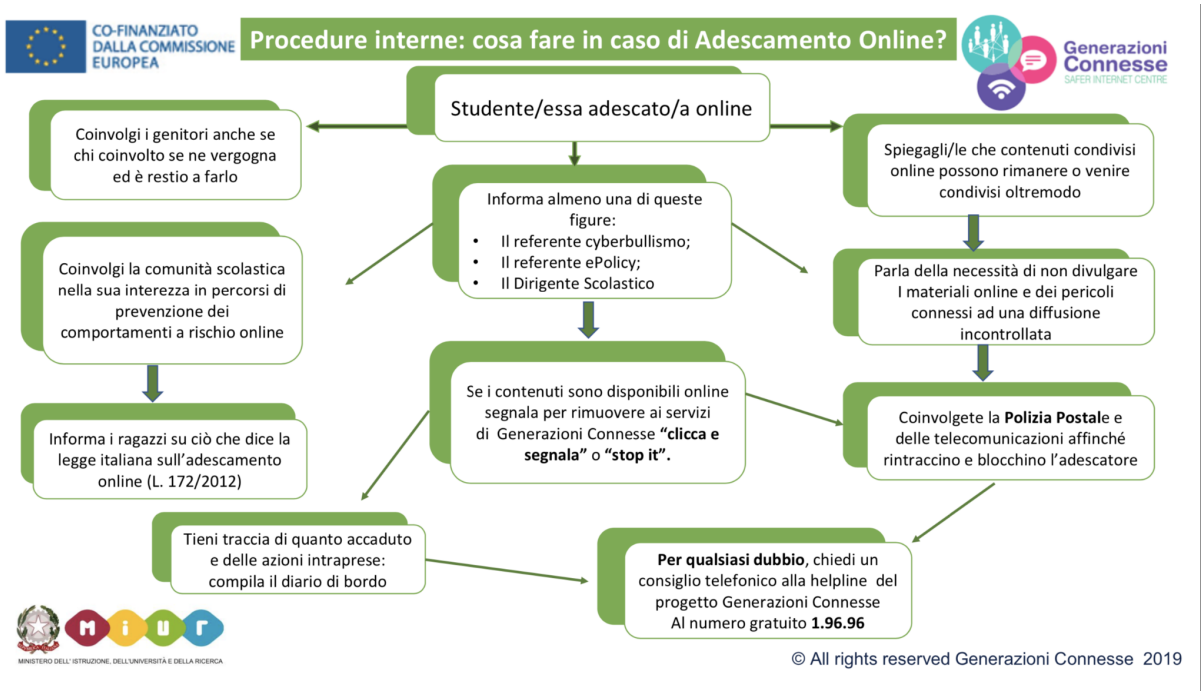
5.4. - Allegati con le procedure
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



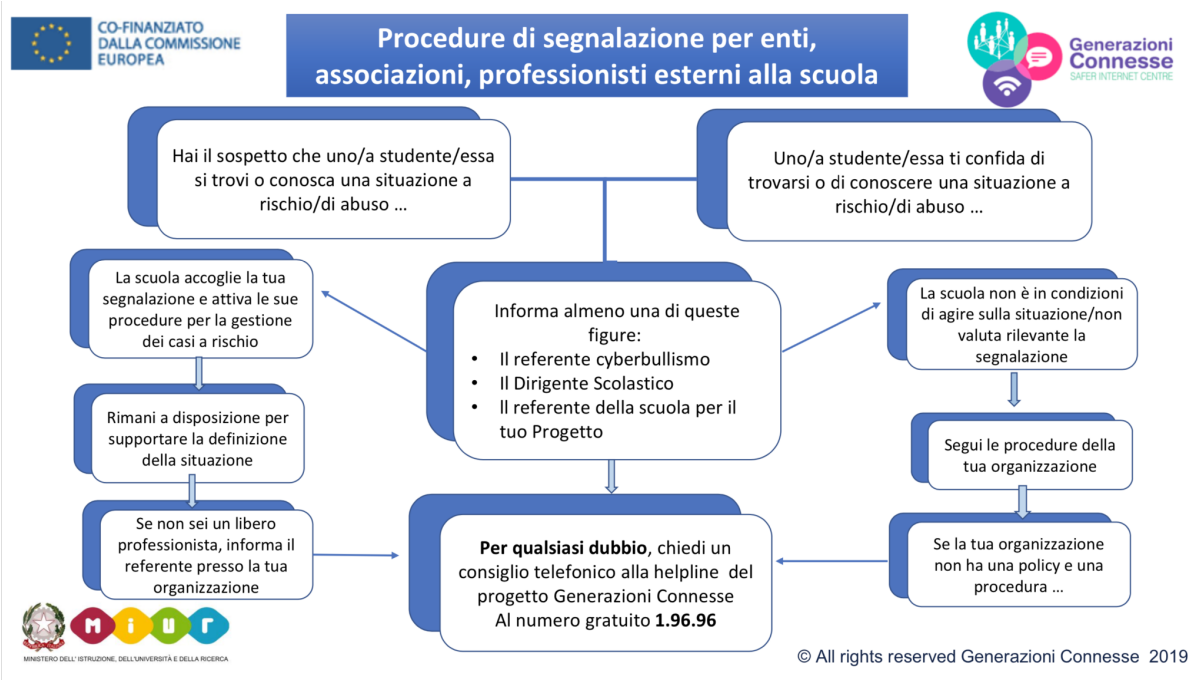
Procedure interne: cosa fare in caso di sexting?



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

5.4. - Allegati con le procedure

Si allegano:

- scheda di segnalazione per casi di bullismo/cyberbullismo
- modello per chiedere l'intervento del Garante per la protezione dei dati personali
- modulo per la segnalazione di casi di bullismo
- modulo per la segnalazione di casi di cyberbullismo
- scheda di valutazione approfondita per casi di bullismo/cyberbullismo
- scheda delle azioni messe in atto e del monitoraggio del percorso

I Referenti per il Bullismo e il Cyberbullismo, in collaborazione con i componenti del Gruppo di ePolicy e dei docenti del cdc coinvolti, compileranno per ogni segnalazione ricevuta e accertata una "Scheda di segnalazione".
Tale scheda sarà aggiornata periodicamente al fine di realizzare un sistematico e proficuo monitoraggio dell'evoluzione della situazione problematica verificatasi.
Inoltre i Referenti per il Bullismo e il Cyberbullismo, in collaborazione con i componenti del Gruppo di ePolicy, compileranno durante l'anno un Diario di Bordo (scheda riepilogativa di tutti i casi che si sono presentati), al fine di realizzare al termine di ogni a.s. una banca dati di riepilogo dei casi verificatisi e delle strategie con cui sono stati affrontati.