Documento di ePolicy

CAIC83900V

I.C. SANLURI

VIA CARLO FELICE - 09025 - SANLURI - CAGLIARI (CA)

CINZIA FENU

Capitolo 1 - Introduzione al documento di ePolicy

1.1 - Scopo dell'ePolicy

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

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

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

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

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

Argomenti del Documento

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

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

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

Perché è importante dotarsi di una E-policy?

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

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

Il documento programmatico dell'e-Policy, elaborato come strumento utile a chiarire l'approccio dell'Istituto rispetto alle tematiche della comunicazione digitale, vuole rappresentare il principale

veicolo di promozione delle azioni formative e informative inerenti la sicurezza nel web promuovendo un uso positivo delle tecnologie digitali nella didattica. Tra gli scopi che l'Istituto si pone con la stesura del presente documento, vi è il preminente interesse a voler attivare e promuovere procedure e protocolli standardizzati per l'utilizzo delle Tecnologie dell'Informazione e della Comunicazione (TIC) in ambiente scolastico con la condivisione delle rispettive norme comportamentali. Parallelamente alle attività di sensibilizzazione all'uso delle TIC nella didattica, si pone come prioritario ed emergente l'interesse a voler sostenere con il documento programmatico dell'e-Policy una serie di azioni e misure volte alla rilevazione e gestione delle problematiche connesse a un uso inconsapevole delle tecnologie digitali e del web; ma anche ad attivare interventi finalizzati alla prevenzione e lotta dei fenomeni collegati al bullismo e cyberbullismo.

Scopo principale del documento Policy di e-safety elaborato dal nostro Istituto è perciò quello di formare/informare tutta la comunità educante sull'utilizzo corretto e responsabile degli strumenti informatici e del web. Le azioni promosse dal piano programmatico sono indirizzate a tutti i membri della comunità scolastica al fine di favorire processi di crescente consapevolezza sui rischi connessi all'esposizione al web e alla navigazione in rete. La Policy di e-safety permette di condividere un sistema di regole e norme di comportamento con i soggetti operanti nell'Istituto e soprattutto con gli alunni affinché siano promosse buone pratiche con l'uso delle TIC e del web dentro la scuola e di riflesso anche fuori dal contesto scolastico. L'e-Policy inoltre regolamenta ed elabora, condividendoli con la comunità educante, i protocolli finalizzati a monitorare ed eventualmente sanzionare comportamenti inappropriati, quand'anche illeciti, avvenuti all'interno dell'istituzione scolastica.

1.2 - Ruoli e responsabilità

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

Considerati i ruoli e le responsabilità delle figure presenti a scuola, come rinvenibili dalla norma (Legge 59/97, Art. 21 CO° 8; Legge N.165/2001 Art. 25; CCNL; DPR n. 275/99; Legge n.107/2015; Piano Nazionale Scuola Digitale), risulta essenziale definire con chiarezza ruoli, compiti e responsabilità dei soggetti che a vario titolo partecipano alla vita scolastica occupandosi della gestione e programmazione delle attività formative, didattiche ed educative dell'Istituto, ma anche di tutte quelle figure appartenenti alla più vasta comunità educante.

Il Dirigente Scolastico

Il Dirigente Scolastico è garante della sicurezza offline e online di tutti i membri della comunità scolastica, in quanto tale ha:

- Il compito di promuove la cultura della sicurezza online e, quando possibile, offrire il proprio

contributo, insieme ai Docenti Referenti del bullismo e cyberbullismo, alla Commissione bullismo-cyberbullismo, all'Animatore Digitale e al Team per l'innovazione digitale, per attivare corsi di formazione specifici indirizzati a tutte le figure scolastiche sull' utilizzo positivo e responsabile delle TIC;
- La responsabilità di gestire e intervenire in tutti i casi di uso improprio delle tecnologie digitali e negli episodi aventi le caratteristiche di bullismo e cyberbullismo come descritte in normativa;
- Il compito di garantire il funzionamento del sistema di monitoraggio e controllo interno della sicurezza on-line;
- Il compito di seguire le procedure previste dalle norme in caso di reclami o attribuzione di responsabilità al personale scolastico in relazione a incidenti occorsi agli alunni nell'utilizzo delle TIC a scuola.

L'Animatore Digitale

L'Animatore digitale con il supporto del Team per l'innovazione digitale, si occupa di supportare il personale scolastico da un punto di vista tecnico-informatico; in tale frangente ricopre anche i seguenti ulteriori compiti e responsabilità:

- Si occupa della pubblicazione della e-Policy sul sito istituzionale della scuola e favorisce la sua conoscenza e diffusione attraverso l'utilizzo dei canali a disposizione;
- Si occupa, in riferimento ai rischi online, di monitorare i livelli di protezione e gestione dei dati personali;
- Promuove percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale coinvolgendo insegnanti, alunni, genitori e altri attori del territorio, nella partecipazione alle attività e ai progetti;
- Effettua il monitoraggio e la rilevazione di eventuali episodi o problematiche connesse all'uso delle TIC a scuola;
- Ha il compito di controllare che gli utenti autorizzati accedano alla Rete della scuola per scopi istituzionali e consentiti (istruzione e formazione);

I Referenti Bullismo e Cyberbullismo

L'Istituto si è adeguato alle disposizioni normative e ministeriali dotandosi di due Referenti che operano in sinergia con la Commissione bullismo e cyberbullismo. I Referenti bullismo e cyberbullismo hanno i seguenti compiti e attribuzioni:

- Coordinare e promuovere iniziative specifiche per la prevenzione e il contrasto dei fenomeni di bullismo e cyberbullismo in collaborazione con altri enti, la Polizia Postale, i canali ministeriali, le campagne di sicurezza… ;
- Garantire la consulenza a tutto il personale dell'Istituto per quanto attiene la gestione delle problematiche di bullismo e cyberbullismo;
- Promuovere la formazione e l'aggiornamento del personale scolastico, la formazione e informazione degli alunni, delle famiglie e di tutta la Comunità Educante rispetto alle problematiche connesse all'uso del web e ai fenomeni di bullismo e cyberbullismo;
- Offrire consulenza e supporto a tutto il personale per le procedure da attivare in caso di

infrazione della e-policy;
- Predisporre materiali utili ai docenti per le attività didattico-formative con gli allievi volte alla sensibilizzazione e prevenzione dei fenomeni di bullismo e cyberbullismo;
- Effettuare il monitoraggio e la rilevazione di eventuali episodi o problematiche connesse a fenomeni di bullismo e cyberbullismo a scuola;
- Effettuare la prima presa in carico attraverso i protocolli formali di episodi categorizzabili come attività di bullismo e cyberbullismo a scuola.

I Docenti

I Docenti promuovono, laddove possibile, l'uso delle tecnologie digitali nella didattica e, avendo un ruolo centrale nel diffondere la cultura dell'uso responsabile delle TIC e del web, possono accompagnare e supportare gli studenti e le studentesse nelle attività di apprendimento e nei laboratori che prevedono l'uso della LIM e di altri dispositivi tecnologici che si connettono alla Rete. Perciò Il docente nel libero esercizio della sua professionalità può avvalersi dei seguenti strumenti: postazioni PC, LIM nelle classi e nei laboratori, aula informatica, dispositivi mobili in dotazione all'Istituto… e ne conseguono in particolare i seguenti compiti e responsabilità:

- Informarsi e aggiornarsi sulle problematiche connesse alla sicurezza nell'utilizzo delle TIC e del web, nonché sulla politica di sicurezza adottata dalla scuola con l'e-Policy, rispettandone i regolamenti collegati;
- Guidare gli alunni, nelle lezioni in cui è programmato l'utilizzo del web, all'uso responsabile della rete ricercando idonei siti e percorsi coerenti all'età e alle competenze dei minori, adatti a un utilizzo didattico-formativo;
- Controllare l'uso che viene fatto delle tecnologie digitali, dei dispositivi mobili, delle macchine fotografiche… nelle lezioni e nelle altre attività scolastiche che ne prevedono l'uso a scopi didattici;
- Assicurare la riservatezza dei dati personali trattati ai sensi della normativa vigente;
- Non divulgare le credenziali di accesso agli account (username e password) e/o, nel caso ne sia a conoscenza, alla rete wi-fi;
- Non allontanarsi dalla postazione lasciandola incustodita, se non prima di aver effettuato la disconnessione;
- Non salvare file contenenti dati personali e/o sensibili sulla memoria locale delle postazioni;
- Segnalare prontamente eventuali malfunzionamenti o danneggiamenti delle TIC al Dirigente Scolastico, all'Animatore Digitale o alle Funzioni Strumentali;
- Comunicare ai genitori difficoltà, bisogni o disagi rilevati dagli alunni a scuola e connessi all'utilizzo delle TIC, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo;
- Segnalare al Dirigente Scolastico o ai Referenti per il Bullismo e Cyberbullismo qualsiasi abuso rilevato a scuola nei confronti degli alunni in relazione all'utilizzo delle tecnologie digitali o del web, per l'adozione dei protocolli e delle procedure previste dalla Policy e dalle norme.

Il personale Amministrativo, Tecnico e Ausiliario (ATA)

Il personale Amministrativo, Tecnico e Ausiliario (ATA) svolgendo funzioni miste connesse all'attività

delle istituzioni scolastiche, promuove lo sviluppo della cultura digitale e del rispetto delle norme della privacy. Perciò il personale ATA avrà il compito di:

- Assicurare la riservatezza dei dati personali trattati ai sensi della normativa vigente;
- Partecipare alle attività di formazione e autoformazione in tema di uso sicuro del web, bullismo e cyberbullismo promosse dall'Istituto;
- Segnalare al Dirigente Scolastico, alla stregua dei docenti, la rilevazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo, al fine di favorire i processi di raccolta, verifica e valutazione delle informazioni inerenti possibili casi in merito.

Gli Studenti e le Studentesse

Gli studenti e le studentesse nel loro ruolo centrale di soggetti in formazione, conoscono e rispettano i regolamenti dell'Istituto, sia generali che specifici delle aule di informatica e segnalano al docente di classe eventuali usi impropri della rete e dei dispositivi. Il ruolo degli alunni include inoltre i seguenti compiti:

- essere responsabili, in relazione all'età, al proprio grado di maturità e di apprendimento, per l'utilizzo dei sistemi caratterizzanti le tecnologie digitali, in conformità con quanto richiesto dai docenti e dai regolamenti;
- comprendere l'importanza di adottare buone pratiche volte ad un uso sicuro e responsabile del web quando si utilizzano le tecnologie digitali per non correre i rischi connessi al loro uso improprio;
- Adottare condotte rispettose degli altri anche quando si comunica in rete;
- Non utilizzare la strumentazione della scuola a scopi personali, ludici e/o ricreativi ferma restando la possibilità che lo preveda esplicitamente l'attività didattica proposta;
- Non utilizzare i propri dispositivi esterni personali senza aver previamente acquisito il permesso da parte dell'insegnante che valuterà l'opportunità didattico-formativa del loro uso;
- Richiedere l'aiuto delle figure di riferimento della comunità scolastica in situazioni di difficoltà o bisogno, in relazione all'utilizzo delle tecnologie didattiche o del web;
- Segnalare, in qualità di attori principali del benessere della comunità scolastica, agli organi preposti (Docenti, collaboratori scolastici, docente fiduciario di plesso, Referenti del bullismo/cyberbullismo, Dirigente Scolastico) eventuali atti di bullismo e cyberbullismo di cui sono a conoscenza, consapevoli del fatto che verrà garantita loro la riservatezza di quanto comunicato;
- Creare una comunità educante, con l'ausilio delle figure professionali della scuola, fondata sui principi della Peer Education finalizzata alla disseminazione delle buone pratiche nell'uso del web;
- Partecipare e co-progettare iniziative finalizzate alla prevenzione dei fenomeni di bullismo e cyberbullismo promuovendo l'uso sicuro del web.

I Genitori

La corresponsabilità educativa e formativa, che riguarda sia i genitori che la scuola nel percorso di crescita degli studenti e delle studentesse, pone i genitori in continuità con l'Istituto scolastico e li rende attivi e partecipi nelle azioni di promozione ed educazione sull'uso consapevole delle TIC e

del web. Sono a carico dei genitori e delle famiglie i seguenti compiti e responsabilità:

- Partecipare attivamente alle azioni di formazione/informazione promosse dall'Istituto inerenti le problematiche afferenti all'uso sicuro del web e ai comportamenti sintomatici del bullismo e del cyberbullismo;
- Conoscere e sostenere le azioni messe in campo dall'Istituto relativamente ai temi della prevenzione e lotta ai fenomeni di bullismo/cyberbullismo e collaborare secondo le modalità previste dal Patto di corresponsabilità;
- Conoscere e condividere le sanzioni previste dalla e-Policy, parte integrante del Regolamento d'Istituto, nei casi di bullismo/cyberbullismo e navigazione online a rischio;
- Sostenere la linea di condotta della scuola adottata nei confronti dell'utilizzo delle Tecnologie dell'Informazione e della Comunicazione nella didattica (TIC);
- Seguire gli alunni nello studio a casa adottando i suggerimenti e le condizioni d'uso delle TIC indicate dai docenti, in particolare attivare il controllo parentale nell'utilizzo del PC, di Internet e degli strumenti Smart;
- Concordare e condividere con i docenti linee di intervento coerenti e di carattere educativo in relazione a eventuali problemi derivati da un uso non responsabile, o a rischio, delle tecnologie digitali e del web;
- Fissare delle regole per l'utilizzo del web e tenere sotto controllo l'uso responsabile dei device personali.

Gli Enti educativi esterni e le associazioni

Gli Enti educativi esterni, le associazioni, le cooperative, i professionisti esterni che entrano in relazione con la scuola rappresentano parte della Comunità Educante perciò devono conformarsi alla politica condotta dall'Istituto rispetto all'uso consapevole del web e delle TIC. Ne consegue che si faranno carico dei seguenti compiti e responsabilità:

- Conoscere e accettare l'informativa di sintesi dell'e-Policy;
- Promuovere comportamenti sicuri nell'uso del web e assicurare la protezione degli studenti e delle studentesse durante le attività che si svolgono insieme;
- Seguire le procedure di segnalazione di qualsiasi abuso rilevato a scuola nei confronti degli alunni in relazione all'utilizzo delle tecnologie digitali o del web, per l'adozione dei protocolli e delle procedure previste dalla Policy e dalle norme.

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).

Il documento dell'e-Policy viene elaborato anche in un formato sintetico denotandolo come informativa da condividere e indirizzare agli enti, organizzazioni, associazioni extrascolastiche e agli esperti esterni chiamati, a vario titolo, nella realizzazione di progetti ed attività didattico-educative a breve, medio e/o lungo termine. L'informativa sintetica sull'e-Policy, contenente un insieme di regole o norme di comportamento, è comprensiva delle procedure di segnalazione da condividere per rilevare, limitare, contrastare e gestire le problematiche connesse ad un uso inconsapevole delle tecnologie digitali. L'informativa rappresenta una forma di garanzia per l'intera comunità educante e di miglioramento del rapporto fiduciario scuola-famiglia. I protocolli di segnalazione prevedono l'identificazione dei soggetti interni alla scuola cui rivolgersi nel caso si vadano a configurare le ipotesi problematiche richiamate nel documento di sintesi dell'e-policy, perciò i Referenti bullismo e cyberbullismo, l'Animatore Digitale, la Commissione Bullismo e il Team per l'Innovazione Digitale…

Per quanto attine le procedure di segnalazione dei casi si rinvia al Cap. 5.

L'informativa deve essere condivisa e sottoscritta nella stipula di eventuali contratti con personale e associazioni esterne ed eventualmente richiamare il regolamento sull'utilizzo dei dispositivi personali (smartphone, tablet, pc, etc.) e quelli in dotazione della scuola, nonché i regolamenti sulla privacy soprattutto di soggetti minorenni.

Il documento di sintesi dell'e-policy, redatto nei termini di informativa per i soggetti esterni che a vario titolo intervengono nella formazione ed educazione degli alunni, prevede la presenza dei seguenti elementi essenziali:

- Premessa e obiettivi dell'informativa;
- Destinatari (i soggetti esterni);
- Ambiti di applicazione (il progetto specifico o delle attività);
- Ruoli (individuare i docenti di riferimento del progetto specifico o delle attività);
- Regolamento;
- Procedure di segnalazione per i soggetti esterni (Protocolli e moduli di segnalazione per le situazioni di rischio);
- Provvedimenti nel caso di omessa segnalazione (a carico dei soggetti esterni);

- Provvedimenti nel caso di comportamenti in violazione del codice di comportamento.

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

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

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

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

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

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

Il documento integrale dell' e-Policy viene pubblicato sulla Home Page del sito istituzionale della scuola dopo essere stato approvato dal Collegio dei Docenti e condiviso con la comunità educante. All'inizio di ogni anno scolastico, l'e-Policy verrà condivisa e illustrata ai genitori e agli alunni, insieme al Patto di Corresponsabilità Educativa.

Il documento di e-Policy viene trasmesso a tutto il personale e alle famiglie per presa visione tramite il registro elettronico in apposita area dedicata e bacheca.

Si prevede la realizzazione di due versioni child friendly del documento di e-Policy, una indirizzata ai bambini/e della Scuola Primaria e una ai ragazzi/e della Scuola Secondaria per la comunicazione e sensibilizzazione degli alunni/e alle problematiche connesse alla sicurezza sul web. La condivisione dei contenuti della Policy verrà svolta annualmente, in occasione del mese della sicurezza in rete, con attività ed eventi strutturati ad hoc tramite l'uso di plurimi linguaggi, mediatori didattici, canali comunicativi, strumenti e tecnologie veicolari e attività didattico-formative adeguati all'età e alle competenze degli utenti.

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.

Componente alunni

Per la componente alunni, le infrazioni verranno sanzionate come da Regolamento di Istituto pubblicato sul sito web della scuola con il quale l'e-Policy si armonizza.

Nel caso in cui un docente rilevi un'infrazione alle indicazioni della Policy è necessario che informi il coordinatore di classe, il quale a sua volta riferisce al Dirigente Scolastico e alla famiglia.

Le potenziali infrazioni in cui è possibile che gli alunni incorrano a scuola nell'utilizzo delle tecnologie digitali e del web sono:

- Un uso della rete per giudicare, infastidire o impedire a qualcuno di esprimersi o partecipare liberamente;
- L'invio non autorizzato di foto o di altri dati sensibili personali come l'indirizzo di casa o il telefono;
- La condivisione di immagini intime;
- La comunicazione incauta e senza permesso con sconosciuti;
- Il collegamento a siti web non espressamente indicati dai docenti e potenzialmente pericolosi.

Nel caso di infrazione della Policy, il Dirigente Scolastico ha la facoltà di revocare l'accessibilità temporanea o permanente ai laboratori informatici e/o all'utilizzo di strumenti tecnologici (pc, tablet, notebook..) di chi non si attiene alle regole stabilite. Sono previsti da parte dei docenti provvedimenti "disciplinari" proporzionati all'età e alla gravità del comportamento, quali:

- Il richiamo verbale;
- Il richiamo verbale con particolari conseguenze (riduzione o sospensione dell'attività gratificante);
- Il richiamo scritto con annotazione sul diario e sul registro elettronico;
- La convocazione dei genitori da parte degli Insegnanti;
- La convocazione dei genitori da parte del Dirigente Scolastico.

I genitori sono invitati a supportare la scuola per mettere a punto azioni di contrasto efficaci.

Gli interventi correttivi previsti per gli alunni sono coerenti con quanto definito nel Regolamento d'Istituto. Nel caso in cui l'infrazione si configuri come atto di bullismo/cyberbullismo, il docente è tenuto a informare immediatamente il Dirigente e i Referenti per il bullismo e cyberbullismo. Si ricorda inoltre che, nel momento in cui un qualunque attore della comunità scolastica venga a conoscenza di un reato perseguibile d'ufficio, è fatto obbligo di denuncia (ex art. 331 del codice di procedura penale). L'omissione di denuncia costituisce reato (art. 361). Nel caso si tratti di un reato è necessario che il Dirigente Scolastico informi le autorità competenti (Polizia Postale) e attivi i

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

I reati riferiti all'ambito digitale e commessi per via telematica che necessitano di immediata attività di tutela della vittima con l'avvio di specifiche procedure, di cui si dà conto al cap.5 dell'e-Policy, sono raggruppabili principalmente in tre categorie:

1. Cyberbullismo;
2. Adescamento on line;
3. Sexting.

Componente Docenti e Personale Scolastico

Le potenziali infrazioni a carico del personale scolastico sono identificabili ne:

- Il trattamento dei dati personali, comuni e sensibili degli alunni, non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi;
- La diffusione delle password assegnate per la navigazione online attraverso la rete della scuola;
- L'uso improprio della strumentazione tecnologica e del web a fini non specificamente didattici e formativi.

Per quanto attiene la componente docenti, le infrazioni alla e-Policy saranno gestite direttamente dal Dirigente Scolastico.

1.6 - Integrazione dell'ePolicy con Regolamenti esistenti

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

Il documento dell'E-Policy dell'Istituto Comprensivo Sanluri si integra pienamente per obiettivi e contenuti con il PTOF e con il PNSD; verrà inoltre armonizzato con il Regolamento di Istituto, con i Regolamenti inerenti l'uso delle TIC, le aule informatiche e la DaD (Didattica a Distanza)e con il Patto di Corresponsabilità Educativa.

1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

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

Il Dirigente Scolastico è responsabile dell'implementazione della Policy all'interno dell'Istituto e si occuperà assieme ai Referenti per il Bullismo e il Cyberbullismo delle rispettive attività di monitoraggio dell'implementazione. L'Animatore Digitale (insieme al Team dell'Innovazione Digitale) e i Referenti per il Bullismo e il Cyberbullismo (insieme alla Commissione Bullismo e Cyberbullismo) in accordo con il Dirigente Scolastico, partecipano alla revisione e all'aggiornamento del documento che dovrà sempre essere sottoposto all'approvazione del Collegio dei Docenti. Si avranno inoltre degli aggiornamenti, laddove necessario e secondo una logica di condivisione e partecipazione attiva, sentito il parere degli insegnanti e viste le esigenze delle famiglie e dei ragazzi.

Il nostro piano d'azioni

AZIONI da svolgere nell'annualità scolastica 2019/2020:

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

AZIONI da svolgere nei prossimi 3 anni:

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

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

Capitolo 2 - Formazione e curricolo

2.1. Curricolo sulle competenze digitali per gli studenti

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

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

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

Le TIC e l'uso del web rappresentano un elemento essenziale per la mediazione, diffusione e disseminazione della conoscenza; essi risultano elementi cardine per favorire i processi dell'apprendimento nella scuola di oggi e di domani. Perciò la scuola ha il dovere di fornire alla componente studentesca l'accesso a questi strumenti come parte della loro esperienza di apprendimento e di far maturare in loro le competenze per una proficua cittadinanza digitale.

L'uso delle TIC è stato inserito dall'Istituto nel curricolo sia a livello disciplinare sia a livello interdisciplinare. In particolare il curricolo è stato strutturato per prevedere il raggiungimento delle competenze digitali di base al termine del primo ciclo secondo i seguenti profili: per la scuola primaria viene orientata un'attività in grado di far sì che l'alunno possa *usare le tecnologie in contesti comunicativi concreti per ricercare dati e informazioni e per interagire con soggetti diversi;* per la Scuola Secondaria di I grado viene condotta un'attività didattico-formativa che permetta all'alunno di *raggiungere buone competenze digitali nell'usare con consapevolezza le tecnologie della comunicazione per ricercare e analizzare dati ed informazioni, per distinguere informazioni attendibili da quelle che necessitano di approfondimento, di controllo e di verifica e per interagire con soggetti diversi nel mondo.*

L'Istituto attraverso il lavoro dei Dipartimenti sta ponendo le basi per la costruzione del Curricolo Verticale, partendo dalla già esistente progettualità verticale tra la Scuola Primaria e Secondaria inerente l'ambito musicale; in tale frangente si andrà a revisionare anche l'area delle competenze digitali predisponendo uno specifico curricolo digitale verticale che allo stato attuale è orientato esclusivamente da quanto dettato dalle indicazioni nazionali.

La competenza digitale è una delle competenze chiave europee, così come si evince dalla Raccomandazione del Parlamento Europeo e del Consiglio (del 18.12.2006/962/CE), nonché dalle Indicazioni nazionali del curricolo n.254/2012 e nuovi scenari (nota MIUR del 1 marzo 2018), in cui si definisce la competenza digitale nei seguenti termini: *"saper utilizzare con dimestichezza e spirito critico le tecnologie della società dell'informazione (TSI) per il lavoro, il tempo libero e la comunicazione. Essa è supportata da abilità di base nelle TIC: l'uso del computer per reperire, valutare, conservare, produrre, presentare e scambiare informazioni nonché per comunicare e partecipare a reti collaborative tramite Internet."*

La competenza digitale perciò è una competenza trasversale e nella nostra Scuola tutti i docenti sono chiamati a promuoverla, come richiamata anche dal profilo delle competenze in uscita dalla Scuola Secondaria di I grado che caratterizza il curricolo dell'Istituto. Ciononostante, è vero che alcune discipline si prestano più di altre e che alcune competenze specifiche sembrano interessare soprattutto l'informatica e la tecnologia.

L'Istituto infine persegue, relativamente al curricolo digitale, le recenti indicazioni del PNSD.

Il "nuovo" curricolo digitale sarà strutturato per coinvolgere le classi 3^, 4^ e 5^ Primaria e le classi 1^, 2^ e 3^ Secondaria. Il percorso formativo di base verrà portato avanti e condotto dai docenti interni alla scuola (docenti titolari dell'insegnamento della disciplina Tecnologia e Informatica, nella Scuola Secondaria, e docenti dell'asse scientifico-matematica, nella Scuola Primaria), mentre alcuni percorsi di arricchimento dell'offerta formativa d'ambito (Laboratori e Progetti su competenze digitali e uso del web) rivolti ad una platea più ristretta e/o selezionata, potranno essere condotti, come già è consuetudine fare, da esperti esterni incaricati a titolo non oneroso o oneroso, tramite la ricerca di specifici finanziamenti economici a bando.

L'Istituto si pone l'obiettivo di progettare e successivamente implementare, parallelamente alla definizione del curricolo verticale d'Istituto, il Curricolo delle Competenze Digitali. Esso sarà caratterizzato dallo sviluppo di tematiche digitali chiave distribuite su quattro specifiche aree:

1. **Alfabetizzazione digitale e sviluppo del pensiero computazionale** - Digital Literacy (#14,#15,#16) e coding (#17);
2. **Comunicazione e collaborazione** - Digital Communication;
3. **Creatività digitale** - Digital Creativity;
4. **Cittadinanza digitale e Intelligenza emotiva digitale** - Digital Citizenship e Digital Emotional Intelligence - (salute, sicurezza, diritti, uso e cura della propria "identità digitale") (azioni PNSD #8,#9,#10).

Per ciascuna area saranno identificate specifiche competenze digitali e rispettivi descrittori; così come i livelli di padronanza previsti per ciascuna competenza; infine le rispettive conoscenze e abilità a esse correlate.

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.

Il corpo docente ha partecipato e partecipa a corsi di formazione anche nell'ambito dei piani nazionali. Gli insegnanti aderiscono alle iniziative formative organizzate dall'Istituzione Scolastica e posseggono in linea di massima una buona base di competenze che, nel caso delle figure di sistema, assumono anche carattere specialistico. Il corpo docente si è mostrato in tali circostanze disponibile ad aggiornarsi per mantenere al passo la propria formazione, in rapporto al rinnovo della dotazione multimediale e delle nuove esigenze formative dei discenti.

All'interno dell'istituto, inoltre, si assiste alla condivisione delle conoscenze dei singoli e alla loro disseminazione supportata dall'Animatore Digitale e dal Team dell'Innovazione Digitale; la formazione avviene anche attraverso la fruizione di materiali messi a disposizione dall'Animatore stesso sulle bacheche virtuali, attraverso corsi di aggiornamento online e attraverso attività formative in presenza organizzate dallo stesso Team dell'Innovazione Digitale.

L'istituto si impegna con sistematicità nell'assicurare tempestiva e capillare informazione su corsi, convegni e seminari formativi inerenti le tematiche in oggetto attraverso le comunicazioni istituzionali in bacheca virtuale sul registro elettronico, cercando di facilitare e valorizzare il personale che intende parteciparvi.

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.

Coerentemente con quanto previsto dal PNSD, l'Istituto si avvale dell'Animatore Digitale, che coordina la diffusione dell'innovazione digitale e collabora con il Team per l'Innovazione Digitale, i Referenti Bullismo e Cyberbullismo, la Commissione Bullismo, nonché tutti i soggetti che possono contribuire alla realizzazione degli obiettivi del Piano. Il percorso di formazione specifica dei docenti sull'utilizzo consapevole e sicuro di Internet, ha previsto e continuerà a prevedere momenti di formazione personale e/o collettiva, aggiornamento e autoaggiornamento, legati all'evoluzione rapida delle tecnologie e delle modalità di comunicazione a cui i bambini e i ragazzi accedono con sempre maggior frequenza e in maniera sempre più autonoma.

All'avvio dell'anno scolastico 2019/2020 è stato attivato un percorso di formazione aperto a tutti i docenti dell'Istituto sulle tematiche connesse all'uso consapevole e sicuro del web con azioni di sensibilizzazione alle problematiche di bullismo e cyberbullismo correlate; la formazione è stata tenuta da un esperto esterno di riconosciuta professionalità.

Risulta attivo un gruppo Whatsapp denominato "Docenti Digitali" finalizzato principalmente alla creazione di una comunità di condivisione in cui socializzare buone prassi e accedere a percorsi di formazione e aggiornamento inerenti: competenze digitali, uso sicuro del web, prevenzione dei fenomeni di cyberbullismo, cyber crime…

Nel corso dell'anno scolastico è stato implementato l'utilizzo della piattaforma Microsoft 365 Educational per la didattica, e in particolare l'uso del registro elettronico per la condivisione di materiali e per l'aggiornamento sulle tematiche dell'uso consapevole e sicuro di internet. Sono stati condivisi con i docenti di tutto l'Istituto materiali informativi sulla sicurezza in internet: per l'approfondimento personale, per le attività didattiche con gli studenti e con i genitori; in particolare grazie all'utilizzo e la rielaborazione dei materiali desunti dai link ai siti specializzati www.generazioniconnesse.it e www.piattaformaelisa.it

Inoltre sul sito della scuola è stato creato uno spazio dedicato, rintracciabile alla voce menu PNSD, http://istitutocomprensivosanluri.edu.it/index.php/pnsd dove risultano attivi i link al progetto www.generazioniconnesse.it e quello al progetto "A caccia di Like", percorsi didattico-formativi di prevenzione dei fenomeni di bullismo e cyberbullismo cofinanziati dalla Fondazione Carolina Picchio.

Nel corso dell'a.s. 2019/2020 è stata attivata l'iscrizione dell'Istituto alla piattaforma ministeriale Elisa (formazione E-Learning degli Insegnanti sulle Strategie Antibullismo) che ha permesso di dotare la scuola e i docenti di strumenti per intervenire efficacemente su bullismo e cyberbullismo. La piattaforma ha consentito la partecipazione dei docenti Referenti bullismo e cyberbullismo a un percorso di formazione e aggiornamento professionale conclusosi efficacemente e poi esteso eccezionalmente a ulteriori 3 unità docenti, una per ogni ordine di scuola.

L'iscrizione dell'Istituto alla piattaforma ministeriale Generazioni Connesse e al Safer Internet

Centre ha consentito la validazione dell'Istituto e l'avvio delle azioni di formazione rivolte ai docenti con l'accesso ai percorsi offerti in piattaforma, atti a fornire strumenti per intervenire efficacemente su bullismo e cyberbullismo. I Docenti Referenti hanno concluso efficacemente anche l'azione formativa loro dedicata in piattaforma SIC; inoltre un importante gruppo di docenti ha avviato la formazione su Bullismo e Cyberbullismo offerta nell'ambito del progetto Generazioni Connesse; infine, 6 docenti hanno svolto il percorso formativo orientato all'elaborazione e costruzione del presente documento E-Policy.

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.

Il nostro Istituto ha organizzato già negli anni passati incontri aperti alle famiglie e agli studenti per sensibilizzare docenti, alunni e genitori sui temi della sicurezza online.

Dall'anno scolastico 2018/2019 è stato attivato un percorso di formazione aperto a tutti i genitori degli alunni dell'Istituto sulle tematiche connesse all'uso consapevole e sicuro del web con azioni di sensibilizzazione alle correlate problematiche di bullismo e cyberbullismo; la formazione è stata tenuta da un esperto esterno di riconosciuta professionalità.

A seguito del percorso formativo dedicato, è stato attivato un gruppo Whatsapp denominato "Genitori Digitali" finalizzato principalmente alla creazione di una comunità di condivisione in cui socializzare buone prassi, rischi correlati all'uso improprio del web e percorsi di formazione e aggiornamento inerenti: competenze digitali, uso sicuro della rete, prevenzione dei fenomeni di cyberbullismo, cyber crime…

Sul sito della scuola è stato creato uno spazio dedicato, rintracciabile alla voce menu PNSD http://istitutocomprensivosanluri.edu.it/index.php/pnsd dove risultano attivi i link al progetto www.generazioniconnesse.it e quello al progetto "A caccia di Like", percorsi di prevenzione dei fenomeni di bullismo e cyberbullismo che prevedono anche azioni di sensibilizzazione indirizzate alle

famiglie.

Anche nei prossimi anni si continuerà ad utilizzare questo approccio per la sensibilizzazione delle famiglie, con incontri che offriranno occasione di confronto e discussione sui rischi rappresentati dall'uso dei device e della rete internet senza un'adeguata formazione in merito ai rischi derivanti da un uso inappropriato di tali dispositivi.

La scuola darà inoltre ampia diffusione, tramite pubblicazione sul sito, del presente documento di Policy per consentire alle famiglie una piena conoscenza del regolamento sull'utilizzo delle nuove tecnologie all'interno dell'Istituto e favorire un'attiva collaborazione tra la scuola e le famiglie sui temi della prevenzione dei rischi connessi a un uso inappropriato del digitale.

L'Istituto si impegnerà inoltre, come indicato nelle disposizioni di cui alla L. 29.05.2017 n.71 art. 5 comma 2, ad integrare il Regolamento Scolastico e il Patto di Corresponsabilità Educativa con le indicazioni e i riferimenti alle condotte di cyberbullismo e le rispettive sanzioni disciplinari in aderenza con il presente documento di E-Policy e coerentemente alle indicazioni in esso riportate.

In particolare, il Patto di Corresponsabilità educativa, puntando a rafforzare il rapporto scuola-famiglia e la condivisione dei contenuti e del reciproco rispetto degli impegni in esso richiamati, andrà aggiornato e armonizzato con specifici riferimenti all'uso delle tecnologie digitali e perciò sarà opportuno rendere partecipe la componente genitoriale relativamente ai contenuti dell'E-Policy e al suo piano d'azione.

Il nostro piano d'azioni

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

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

AZIONI da sviluppare nell'arco dei tre anni scolastici successivi

- Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.

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

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

3.1 - Protezione dei dati personali

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

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

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

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

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

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

personali.

Il nostro Istituto osserva il rispetto della privacy dei propri utenti e protegge i dati personali che gli stessi vi conferiscono. I dati personali vengono richiesti solo in caso di effettiva necessità e sono trattati in conformità alla normativa vigente (Decreto legislativo 30 giugno 2003, n. 196, c.d. *Codice della Privacy* armonizzato al *Regolamento UE 2016/679* del Parlamento Europeo e del Consiglio con il D. Lgs. 10 agosto 2018, n. 101 e il GPPR). L'utente è sempre informato sulle finalità della raccolta dei dati personali al momento della stessa fornitura e ne firma, ove necessario, il consenso al trattamento. I dati personali dell'utente non sono comunicati a terzi senza il consenso dello stesso, fatti salvi i casi previsti dalla legge.

Nella fase di iscrizione al nostro Istituto, i genitori degli alunni rilasciano il consenso all'utilizzo di materiale fotografico e audiovisivo per pubblicazioni in formato cartaceo e/o digitale all'interno dell'edificio scolastico e/o nel sito della Scuola o di altre Amministrazioni dello Stato e nelle piattaforme didattiche in uso, in conformità alla normativa vigente e sulla base di quanto espresso nella regolamentazione comunitaria summenzionata.

L'accesso ai dati di ogni singolo alunno, riportati nel registro elettronico (ritardi, assenze, note disciplinari, richiami, annotazioni e valutazioni …), è riservato ai rispettivi genitori tramite l'invio e la gestione di una password di accesso strettamente personale.

Il personale scolastico è "incaricato del trattamento dei dati personali" nei limiti delle operazioni e delle categorie di dati necessarie ai fini dello svolgimento della propria funzione e nello specifico della docenza (istruzione e formazione). Perciò l'Istituto Comprensivo, in riferimento alle finalità istituzionali dell' istruzione e della formazione e a ogni attività a esse strumentale, raccoglie, registra, elabora, conserva e custodisce dati personali identificativi dei soggetti con i quali entra in relazione nell'ambito delle procedure per l'erogazione di servizi formativi. In applicazione del D.Lgs 196/2003 e successive integrazioni, i dati personali sono trattati in modo lecito, secondo correttezza e con adozione di idonee misure di protezione relativamente: all'ambiente in cui vengono custoditi, al sistema adottato per elaborarli, ai soggetti incaricati del trattamento. I dati in nessun caso vengono comunicati a soggetti privati senza il preventivo consenso scritto dell'interessato. Ai soggetti interessati sono riconosciuti il diritto di accesso ai dati personali e gli altri diritti definiti dall'art. 7 del D.Lgs 196/2003 e i diritti sostanziati agli artt. 15,16,17,18,20,21 del GDPR Regolamento UE 679/2016.

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.

Le TIC e l'uso del web rappresentano un elemento essenziale per la mediazione, diffusione e disseminazione della conoscenza; essi risultano elementi cardine per favorire i processi dell'apprendimento nella scuola di oggi e di domani.

L'utilizzo dell'accesso a internet è legato alle esigenze di programmazione didattica e all'espletamento delle pratiche burocratiche. A tal fine si cerca di porre massima attenzione nel:

- Mantenere separate la rete didattica da quella di segreteria al fine di garantire maggiore sicurezza alle informazioni, gestendo in modo autonomo e con regole differenti le due reti;
- Aggiornare periodicamente software e sistema operativo per garantire che il sistema sia aggiornato e protetto dalle aggressioni esterne e dalle vulnerabilità che emergono nel tempo;
- Definire la programmazione di backup periodici per la messa in sicurezza dei dati del sistema scolastico e prevenire la perdita degli stessi;
- Garantire la formazione adeguata dell'Animatore Digitale e del Team dell'Innovazione Digitale per la disseminazione delle conoscenze al corpo docenti su: gestione dei dispositivi e conoscenza delle regole basilari sul loro utilizzo in sicurezza.

La scuola adotta e promuove gli accorgimenti utili a evitare comportamenti contrari a ogni forma di

sicurezza informatica, come: scaricare file video potetti da copyright; accedere a contenuti non adeguati e conformi; alterare parametri di protezione dei device; modificare le impostazioni predefinite dei PC; accedere a siti non finalizzati alla didattica; utilizzare la rete per usi privati e personali … Per garantire che Internet sia uno strumento finalizzato ai soli scopi formativi, verrà esercitato costantemente il monitoraggio e l'aggiornamento dei programmi antivirus e saranno implementati sistemi di filtraggio e di identificazione di contenuti non educativi accessibili on line, certificazioni, blocco di pop-up…

I computer fissi presenti nelle aule e nei laboratori accedono ad Internet attraverso rete LAN. I PC portatili e i tablet in dotazione all'Istituto sono collocabili nelle aule e accedono tramite WIFI. Tutti i PC portatili presenti nella Scuola sono accessibili tramite una password e sono dotati di un antivirus; le LIM delle aule, finalizzate al solo uso didattico, non presentano password d'accesso. I docenti possono accedere con i loro dispositivi personali alla rete WIFI tramite password protetta, gli alunni non possono accedere con i loro dispositivi personali alla rete internet della Scuola. Gli studenti possono accedere ad Internet in aula attraverso l'uso della sola LIM con la supervisione del docente e in occasione di attività didattiche che si svolgono nell'aula del laboratorio informatico su postazione individuale e con accesso tracciato. Nell'attività quotidiana, ogni docente accede al registro elettronico attraverso una password personale che non può essere comunicata a terzi, né agli alunni; il docente si sincera della protezione del proprio account attraverso la corretta uscita dal sistema al termine della sessione di lavoro.

Il sito web dell'Istituto è già opportunamente migrato da suffisso ".gov" a suffisso ".edu" ed è raggiungibile all'indirizzo www.istitutocomprensivosanluri.edu.it , i suoi contenuti vengono curati dal referente del sito web e Animatore Digitale supportato dalle Funzioni Strumentali per l'Informatica, dal Dirigente Scolastico e dalla Segreteria.

Tutti i docenti e gli alunni dell'istituto possiedono una e-mail della scuola del tipo: nome.cognome@CAIC83900v.onmicrosoft.com finalizzata all'utilizzo della piattaforma didattico-formativa multimediale nelle attività di DaD (Didattica a Distanza). La dotazione di indirizzi di posta elettronica sia dei docenti che degli alunni appartiene all'infrastruttura Microsoft 365 Education.

Il nostro Istituto regolamenta le attività di E-Learning previste nella DaD attraverso il documento delle "Linee Guida sulla Didattica a Distanza"; inoltre questo, al suo interno, disciplina l'uso e l'autorizzazione alla fruizione di differenti strumenti per il distance learning e le piattaforme educative in uso, regola il comportamento da tenere in occasione della partecipazione alle sessioni di formazione online e in videoconferenza.

Il nostro Istituto disciplina l'utilizzo del Laboratorio Informatico attraverso uno specifico Regolamento sull'uso delle aule informatiche, armonizzato con le indicazioni presenti nel più generale Regolamento d'Istituto.

3.3 - Strumenti di comunicazione online

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

Il nostro Istituto promuove appieno l'utilizzo di strumenti di comunicazione online sia tra il personale della scuola che tra la scuola e la famiglia e, dall'anno scolastico 2019/2020, in maniera capillare anche nella comunicazione didattica docente-allievi e allievi-allievi con l'introduzione della DaD unificata e regolamentata da specifiche linee guida .

I docenti dell'Istituto utilizzano tutti con sistematicità il registro elettronico, un numero sempre maggiore di essi fruisce appieno delle sue potenzialità rendendo immediate, trasparenti ed efficaci le comunicazioni all'interno della scuola e fra scuola e famiglia. La totalità dei docenti utilizzano lo strumento del Registro Elettronico per la registrazione, trasmissione, e condivisione con specifiche utenze dei seguenti contenuti:

- Andamento scolastico (assenze, argomenti lezioni e compiti, note disciplinari …);
- Programmazione didattico-disciplinare (programmazione annuale, settimanale, progetti …);
- Risultati scolastici (voti, documenti di valutazione …);
- Udienze (prenotazioni colloqui individuali, incontri scuola-famiglia …);
- Eventi (agenda eventi, manifestazioni, seminari, incontri formativi, uscite didattiche …);
- Comunicazione varie (comunicazioni di classe, comunicazioni personali …);
- Bacheca didattica (condivisione contenuti e materiali didattici con docenti, allievi e famiglie);
- Condivisione e disseminazione di saperi e conoscenze (link utili per formazione e aggiornamento, caricamento materiali utili per la didattica …);
- Comunicazioni istituzionali formali con o senza presa visione (circolari, avvisi, comunicati …)

Sarebbe opportuno riuscire ad estendere l'utilizzo del registro elettronico come piattaforma deputata alla mediazione della comunicazione, dell'apprendimento e della formazione rendendone universali l'uso e la fruizione da parte di tutta la comunità educante.

L'Istituto promuove l'uso di strumenti di comunicazione esterna investendo in primis sul sito web istituzionale. Tramite opportuni collegamenti, da questo di accede a specifici canali cui l'Istituto è collegato in vista di attività e progetti a forte valenza educativa e comunicativa, a titolo esemplificativo ma non esaustivo: Accesso Registro Elettronico Argo; e-Twinning; Blog della scuola; Progetto Generazioniconnesse; Progetto A scuola di Like; DislessiAmica ….

Nelle attività didattico-formative in distance learning, da marzo 2020 l'Istituto ha dotato tutti i docenti e gli alunni dell'istituto di una e-mail della scuola del tipo: nome.cognome@CAIC83900v.onmicrosoft.com finalizzata all'utilizzo del potente strumento di comunicazione online offerto dalla piattaforma multimediale dedicata alla DaD (Didattica a Distanza) la cui infrastruttura gestionale è di Microsoft 365 Education. Inoltre, risultavano già attive, e permangono, numerose esperienze di didattica mediata da strumenti di facilitazione e comunicazione online con l'uso di social network come Youtube, Skype, Whatsapp o con l'utilizzo di piattaforme per l'e-learning sincrono e asincrono come We School, Teams, Edmodo. L'utilizzo di tali

strumenti è stato regolamentato dal documento d'Istituto con le "Linee guida per la Didattica a Distanza".

3.4 - Strumentazione personale

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

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

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

Genericamente gli studenti non possono utilizzare i propri dispositivi durante le attività didattiche come previsto dal regolamento disciplinare, né possono accedere alla rete attraverso i dispositivi della scuola se non previa autorizzazione del docente presente in aula e comunque per l'arricchimento di percorsi e attività didattico-formative proposti nell'ambito delle azioni d'aula. Inoltre, agli alunni non è consentito l'uso e l'accesso alla rete WI-FI protetta da password. È consentito ai soli alunni in difficoltà, DSA e BES, l'utilizzo sistematico del proprio tablet o notebook, con l'adeguata supervisione del docente. È consentito a tutti gli alunni, in casi specifici concordati con il docente (laboratori informatici, percorsi didattici strutturati, uscite didattiche, produzioni multimediali...), l'utilizzo di dispostivi elettronici personali per scopi didattici e finalità previamente stabilite. Tuttavia, anche il nostro Istituto vuole promuovere in collaborazione con i docenti un cambiamento d'approccio per quanto attiene l'utilizzo dei device personali introducendo il BYOD, letteralmente "porta il tuo dispositivo"; espressione che descrive quelle politiche aziendali che in tutto il mondo consentono agli impiegati di utilizzare i propri dispositivi personali in ambiente di lavoro. In tal senso, i PC, i tablet e gli smartphone personali potranno essere normalmente integrati nel lavoro in classe allorquando questo risulti ben progettato e calibrato per discipline e obiettivi didattico-formativi.

Gli insegnanti possono utilizzare i dispositivi della scuola per realizzare tutte le attività connesse alla funzione docente. E' consentito loro l'uso in classe dei propri dispositivi per quanto attiene l'attività didattica e qualora risultino necessari, ma non possono essere utilizzati durante le lezioni per questioni strettamente personali. I docenti accedono liberamente al web tramite WI-FI dell'Istituto

con password protetta. Durante il restante orario di servizio è consentito loro l'utilizzo del cellulare solo per comunicazioni personali di carattere "urgente". Al restante personale scolastico non è consentito, durante l'orario di servizio, l'utilizzo di device personali per usi che esulino dal ruolo professionale ricoperto e soprattutto che possano configurarsi come strettamente personali. È consentito l'utilizzo del telefono cellulare o smartphone solo per comunicazioni personali caratterizzate da reale urgenza e contingenza.

Il nostro piano d'azioni

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

- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

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

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli studenti e delle studentesse
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte dei docenti
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte del personale Tecnico Amministrativo e dagli ATA
- Organizzare uno o più eventi o attività volti a consultare i docenti, il personale, le famiglie gli studenti dell'Istituto per redigere e integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali
- Organizzare uno o più eventi o attività volti a formare il personale adulto, gli studenti e i genitori dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali

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

4.1 - Sensibilizzazione e Prevenzione

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

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

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

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

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

La comunità educante che opera nella e per la scuola, e in particolare il corpo docente, è chiamato nell'urgenza dell'utilizzo generalizzato e diffuso delle tecnologie e del web ad assumere il ruolo di "supervisore" individuando tempestivamente le problematiche e i rischi che bambini e adolescenti possono trovarsi ad affrontare ogni giorno. La prima responsabilità degli insegnanti consiste, dunque, nell'imparare a riconoscere i rischi più comuni in cui i ragazzi possono incorrere sul web, per poter poi intervenire adeguatamente. Tra questi, un'attenzione speciale andrà prestata ai fenomeni di bullismo e cyberbullismo. Per questo motivo il nostro Istituto promuove azioni di sensibilizzazione alle problematiche connesse all'uso improprio e inconsapevole del web da parte di bambini e ragazzi attivando:

- Percorsi di formazione tramite i canali istituzionali ministeriali di www.generazioniconnesse.it e www.piattaformaelisa.it ;
- Percorsi di formazione e aggiornamento condotti da esperti esterni;
- Condivisione di materiali e percorsi per l'autoformazione in presenza e a distanza.

La classe è un osservatorio privilegiato della relazione che l'alunno intrattiene con i pari e con il mondo adulto; spesso il docente assume l'inevitabile ruolo di confidente che accoglie le esperienze dei minori accompagnandoli nella costruzione dialogica di un percorso formativo partecipato. Questo substrato connaturato al sistema scolastico, facilita la progettazione e implementazione di percorsi di sensibilizzazione e prevenzione che devono essere indirizzati a tutta la comunità educante e a tutti gli alunni dell'Istituto, sin da piccoli, con percorsi misurati all'età e alle esigenze rilevate/rilevabili.

Fondamentale è quindi il monitoraggio costante delle relazioni interne alla classe, finalizzato a individuare possibili situazioni di disagio su cui intervenire tempestivamente, anche mediante il ricorso alle figure di sistema specializzate, per sostenere il singolo nelle situazioni di difficoltà personale e indirizzare il gruppo verso l'instaurazione di un clima positivo, di reciproca accettazione e rispetto, nelle situazioni di difficoltà socio-relazionali.

Tale percorso interno viene ulteriormente rinforzato dalla partecipazione a progetti e/o iniziative esterne coerenti con i rischi riferiti sotto, cui la scuola porrà particolare attenzione, progettando, promuovendo o selezionando iniziative significative con Enti, Associazioni, Esperti di comprovata esprienza e affidabilità.

Tra i principali rischi derivanti dall'uso inconsapevole delle TIC e del web vanno ricordati:

- La possibile esposizione a contenuti violenti e non adatti all'età degli alunni;
- Videogiochi diseducativi integrati a contenuti inadatti all'età;
- Pubblicità ingannevoli che veicolano e mediano comportamenti anti-sociali;
- Accesso ad informazioni, foto e video che mediano contenuti diseducanti e scorretti;
- Virus informatici in grado di infettare i device e orientare un uso scorretto del web;
- Possibili contatti con adulti che vogliono conoscere e avvicinare bambini/e o ragazzi/e attivando fenomeni di grooming (adescamento on-line);
- Rischi derivati da molestie e/o maltrattamenti attivati da coetanei (cyberbullismo);
- Contatto con materiale a sfondo sessuale e attivazione di scambio di immagini compromettenti (sexting);
- Utilizzo eccessivo di device collegati alla rete con sviluppo di forme di dipendenza da gioco.

Il nostro Istituto riconosce l'importanza di identificare e prevenire tutti questi fenomeni legati all'uso inconsapevole della Rete Internet e ritiene essenziale porre in campo una serie di azioni e strategie indirizzate a sensibilizzare e parallelamente prevenire l'insorgenza degli stessi.

L'Istituto ha attivato e continuerà a condurre iniziative volte alla sensibilizzazione e prevenzione dei fenomeni sopra richiamati attraverso le seguenti azioni:

SCUOLA DELL'INFANZIA

Percorsi di educazione socio-affettiva ed emotiva; laboratori centrati sul riconoscimento delle emozioni; educazione all'ascolto e alla cura; attivazione del progetto di prevenzione d'Istituto "A caccia di Like" cofinanziato dalla Fondazione Carolina Picchio.

SCUOLA PRIMARIA E SCUOLA SECONDARIA DI I GRADO

Percorsi di educazione socio-affettiva ed emotiva; laboratori centrati sul riconoscimento e la gestione delle emozioni; educazione all'ascolto e alla cura; percorsi progressivi per lo sviluppo delle competenze di empatia e accoglienza dell'altro. Dalla classe terza primaria vengono inoltre attivati i percorsi di promozione delle competenze digitali che saranno successivamente armonizzati al "nuovo curricolo verticale digitale" accompagnando l'allievo sino al termine del primo ciclo d'istruzione. Inoltre, vengono attivate e riproposte nel triennio programmatico le seguenti azioni di sensibilizzazione e prevenzione:

- La giornata del Safer Internet Day e il mese della sicurezza sul web;
- I percorsi di sensibilizzazione all'uso sicuro e consapevole del web tenuti dai docenti formati disponibili nell'Istituto;
- I percorsi formativi, di orientamento e aggiornamento, di sensibilizzazione all'uso sicuro e consapevole del web disponibili sul canale www.generazioniconnesse.it ;
- I percorsi di sensibilizzazione all'uso sicuro e consapevole del web tenuti da Esperti esterni, dalla Polizia Postale, dai Carabinieri, dal Garante Regionale per l'Infanzia e l'Adolescenza;
- Il progetto di prevenzione d'Istituto "A caccia di Like" cofinanziato dalla Fondazione Carolina Picchio;
- Tutte le altre iniziative, a bando e non, che verranno promosse in itinere da Enti esterni.

L'intera attività preventiva sarà sempre caratterizzata da azioni rivolte a tutte le utenze dell'Istituto e all'intera comunità educante, consci del fatto che gli interventi di sistema rappresentano la formula vincente nella prevenzione universale.

Le azioni programmatiche saranno progettate come di consueto su tre linee preventive:

- **Prevenzione Universale** che prevede un programma rivolto a tutti gli studenti in quanto soggetti potenzialmente a rischio. Si tratta quindi di interventi d'Istituto, o di grado di scuola, che cercano di raggiungere tutte le utenze sensibilizzando a problematiche collegate all'uso inconsapevole del web e che parallelamente sviluppano competenze su grandi gruppi; quelle competenze educative di base necessarie a poter gestire le situazioni di vita che i/le ragazzi/e sperimentano online.
- **Prevenzione Selettiva** che rappresenta quei programmi indirizzati ad un gruppo di studenti in cui è stato rilevato il rischio online tramite precedenti indagini e segnalazioni fatte dalla scuola. In questi casi gli interventi sono mirati e prevedono programmi formativi strutturati ad hoc e all'occorrenza con l'obiettivo generale di migliorare le competenze digitali e le strategie di problem solving di un gruppo ristretto.
- **Prevenzione Indicata** che accoglie quei programmi di intervento sul caso specifico, pensati e strutturati per ridimensionare e ridurre il danno dei comportamenti problematici rilevati, oppure dare supporto alle vittime. Per sua natura, questo tipo di intervento multilivello si avvale di plurime professionalità, dei servizi socio-sanitari e talvolta giuridici, con l'opportuno

coinvolgimento anche della famiglia dell'alunno/a.

I programmi di Prevenzione Universale sono quelli su cui il nostro Istituto orienta maggiormente le proprie forze, che progetta e realizza con maggiore frequenza, in modo da dover conseguentemente attuare una quantità certamente contenuta di misure preventive di tipo selettivo e indicato.

4.2 - Cyberbullismo: che cos'è e come prevenirlo

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

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

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

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

Il cyberbullismo è una forma di prepotenza virtuale messa in atto attraverso l'uso della rete Internet e delle tecnologie digitali. Spesso i termini bullismo e cyberbullismo vengono usati impropriamente

riconducendo a essi i più svariati episodi di violenza o offese fra ragazzi. Bullismo e cyberbullismo hanno, però, caratteristiche ben precise e non vanno confusi con altre problematiche relazionali.

Il termine cyberbullismo viene coniato da Bill Belsey nel 2002, ma una prima vera definizione del fenomeno viene elaborata solo qualche anno dopo. Nel 2006 Smith e collaboratori definirono il cyberbullismo come: "Un atto aggressivo e intenzionale perpetrato da un individuo o da un gruppo, attraverso l'uso delle nuove tecnologie della comunicazione, in modo ripetuto e continuato nel tempo, contro una vittima che non può facilmente difendersi". Tuttavia, la definizione di cyberbullismo fornita dalla Legge 71/2017 "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo" rappresenta la formula meglio compiuta e argomentata del fenomeno. Non dobbiamo dimenticare che, sia nel cyberbullismo che nel bullismo, si parla di abusi e prevaricazioni che coinvolgono solamente minori con un'importante differenza nelle forme di "potere" messe in gioco. Il cyberbullismo si concretizza infatti nel "potere digitale" che denota l'asimmetria di potere tra cyberbullo e cybervittima.

Il cyberbullismo si caratterizza anche per ulteriori tratti specifici che lo distinguono dal bullismo tradizionale per via delle tecnologie digitali coinvolte, essi sono:

- **L'impatto**, che consta della caratterizzazione virale propria della rete e permette la diffusione di materiale offensivo o denigratorio in maniera incontrollata, illimitata, in grado di distruggere la reputazione della vittima;
- **La convinzione dell'anonimato**, che abbatte le inibizioni e offre un delirio di potere ai cyberbulli i quali si sentono autorizzati a offendere e denigrare online le vittime nella convinzione di non essere identificabili;
- **L'assenza di confini spaziali**, grazie a cui il cyberbullo agisce sapendo di poter arrivare virtualmente ovunque, invadendo anche gli spazi personali della vittima che vive nella consapevole impotenza nei confronti delle azioni online di terzi, perpetuate a suo discapito in ogni dove e in ogni quando;
- **L'assenza di limiti temporali dell'atto persecutorio**, che può avvenire a ogni ora del giorno e della notte;
- **L'indebolimento dell'empatia** agita dalla mediazione digitale della relazione, a causa della quale vi è la degenerazione massima dei comportamenti prevaricatori poiché si diventa incapaci di provare e riconoscere le emozioni simili a quelle che provano i vittimizzati;
- **Il feedback non tangibile,** ovvero l'impercettibilità delle reazioni differite della vittima che riducono ulteriormente i livelli di empatia e il riconoscimento del danno provocato.

Il cyberbullismo si perpetra in un contesto virtuale che spesso viene letto come non "reale", al massimo come una parentesi ludica della realtà. Se per un verso la lettura di comportamenti offensivi, o genericamente problematici vengono troppo frettolosamente catalogati come atti di bullismo, di converso il fenomeno del cyberbullismo è troppo di frequente sottovalutato anche dal mondo adulto, familiare e scolastico, proprio per il suo "carattere virtuale". La mediazione tecnologica porta a un indebolimento del controllo morale personale, con la conseguente pericolosa minimizzazione delle responsabilità individuali.

Diventa necessario a tal proposito lavorare e offrire opportunità e percorsi didattico-formativi affinché le nuove generazioni che si approcciano al digitale, da subito abbiano ben chiaro che:

- Virtuale equivale a reale;
- Il virtuale è governato dalle medesime regole sociali e morali della vita quotidiana;
- Fingere di essere altri non significa esserlo per davvero, la propria identità rimane ed è sempre rinvenibile;
- Il contesto virtuale non è un mondo ludico di fantasia e gioco, ma è il mondo reale;
- L'unico responsabile del danno perpetrato nei confronti della vittima non è solamente il cyberbullo ma anche il commentatore, l'incitatore, l'osservatore passivo che tace pur sapendo.

Il nostro Istituto, nella consapevolezza della dimensione sociale e gruppale del fenomeno, ritiene opportuno portare avanti una serie di azioni finalizzate innanzitutto alla sua prevenzione come già descritte al paragrafo 4.1. "Sensibilizzazione e Prevenzione"

Nello specifico, avendo presenti le indicazioni normative della L.71/2017 e le rispettive linee di orientamento per la prevenzione e il contrasto del cyberbullismo", l'Istituto Comprensivo Sanluri sta conducendo e intende portare avanti le seguenti azioni e attività dedicate:

- Scelta e nomina di due referenti bullismo e cyberbullismo per l'Istituto, rispettiva formazione tramite i percorsi offerti da www.generazioniconnesse.it e www.piattaformaelisa.it cui è seguita l'attribuzione del coordinamento di tutte le iniziative inerenti le attività di prevenzione e contrasto dei fenomeni in oggetto;
- Formazione del personale scolastico attraverso i percorsi offerti da www.generazioniconnesse.it e www.piattaformaelisa.it; corsi di aggiornamento e formazione tenuti da esperti esterni a contratto; incontri e seminari tenuti in collaborazione con la Polizia Postale, i Carabinieri, il Garante Regionale per l'Infanzia e l'Adolescenza; attività di autoformazione e autoaggiornamento con disseminazione delle opportunità formative e delle conoscenze acquisite;
- Formazione dedicata agli alunni dell'Istituto attraverso l'utilizzo degli strumenti e dei contenuti offerti da www.generazioniconnesse.it e www.piattaformaelisa.it; corsi di formazione tenuti da esperti esterni a contratto; incontri, dibattiti e seminari tenuti in collaborazione con la Polizia Postale, i Carabinieri, il Garante Regionale per l'Infanzia e l'Adolescenza; Laboratori e percorsi didattico-formativi a tema …
- Sviluppo delle competenze digitali del personale scolastico, attraverso specifiche iniziative di formazione e aggiornamento proposte dall'Animatore Digitale e dal Team per l'Innovazione Digitale;
- Sviluppo generale delle competenze digitali degli alunni dell'Istituto attraverso la definizione del "nuovo" curricolo digitale verticale; attivazione di specifiche iniziative, azioni, progetti e laboratori didattico-formativi inerenti i temi del digitale;
- Promozione di percorsi e progetti, anche a bando, che prevedono un ruolo attivo degli studenti in attività di peer education e peer to peer;
- Previsione di misure di sostegno e rieducazione dei minori coinvolti in fenomeni di bullismo/cyberbullismo in stretta collaborazione con i servizi socio-sanitari e l'associazionismo locale;
- Aggiornamento, integrazione e armonizzazione all'E-Policy dei Regolamenti e del Patto di Corresponsabilità Educativa con specifici riferimenti alle condotte di cyberbullismo e rimandi

alle rispettive sanzioni disciplinari.

Le modalità di segnalazione e gestione dei casi problematici si rinviano al Capitolo 5 e alle procedure interne ivi segnalate; ci si limita a sottolineare che, salvo il fatto costituisca reato, il Dirigente Scolastico qualora venga a conoscenza di atti di cyberbullismo informa tempestivamente i genitori dei minori coinvolti (art.5). Per quanto riguarda la necessità di segnalazione e rimozione, ciascun minore ultraquattordicenne (o i suoi genitori o chi esercita la responsabilità del minore) che sia stato vittima di cyberbullismo può inoltrare al titolare del trattamento o al gestore del sito internet o del social media un'istanza per l'oscuramento, la rimozione o il blocco dei contenuti diffusi nella Rete. Se entro 24 h il gestore non avrà provveduto, l'interessato può rivolgere analoga richiesta al Garante per la protezione dei dati personali, che rimuoverà i contenuti entro 48 ore. Il Garante ha pubblicato nel proprio sito il modello per la segnalazione/reclamo in materia di cyberbullismo che va inviato a: cyberbullismo@gpdp.it.

Parallelamente, nel caso in cui si ipotizzi che ci si possa trovare di fronte alla fattispecie del reato si potrà far riferimento agli uffici preposti delle Forze di Polizia per inoltrare la segnalazione o denuncia/querela e permettere alle autorità competenti l'approfondimento della situazione da un punto di vista investigativo. In tal caso bisogna far riferimento a uno dei seguenti uffici: Polizia di Stato – Compartimento di Polizia postale e delle Comunicazioni; Questura o Commissariato di P.S. del territorio di competenza; Arma dei Carabinieri – Comando Provinciale o Stazione del territorio di competenza; Polizia di Stato – Commissariato on line (attraverso il portale http:// www.commissariatodips.it).

Per il supporto nella gestione del caso è possibile rivolgersi alla Helpline di Telefono Azzurro.

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.

L'Hate speech è un'espressione tradotta normalmente in italiano come "discorsi d'odio" o "espressioni d'odio" o "linguaggio d'odio" che consiste in una specifica forma di discriminazione che si estrinseca mediante deprecabili modalità di manifestazione in Rete del pensiero. Tali forme espressive, diffuse, amplificate e reiterate attraverso il web, hanno l'effetto di alimentare i pregiudizi, consolidare gli stereotipi e rafforzare l'ostilità nei confronti di gruppi con diverse caratteristiche, in genere minoritarie. L'Hate speech è una degenerazione del cyberbullismo perché non prende di mira una singola vittima, ma delle categorie di individui che sono considerati vulnerabili per alcune caratteristiche: razziali, di orientamento sessuale, religioso, di disabilità.

Per i rischi connessi all'utilizzo delle nuove tecnologie (cyberbullismo, hate speech, grooming, sexting, adescamento online…), il nostro Istituto si affida a consulenti esterni "esperti" come la Polizia Postale, i Carabinieri, il Garante Regionale per l'Infanzia e l'Adolescenza e organizza incontri formativo/informativi rivolti ai docenti, agli alunni e alle famiglie.

Parallelamente, l'Istituto stesso si attiva con le sue risorse umane, durante le ore curricolari o extracurricolari, per attivare percorsi laboratoriali ed esperienziali finalizzati alla sensibilizzazione e prevenzione dei fenomeni suddetti con l'obiettivo di:

- Far maturare e sviluppare le competenze digitali degli allievi;
- Favorire l'educazione ad un uso etico e consapevole delle tecnologie e del web;
- Fornire gli strumenti necessari per prevenire o decostruire stereotipi su cui spesso si fondano forme di hate speech legati alla razza, al genere, all'orientamento sessuale, alla disabilità;
- Promuovere la partecipazione civica e l'impegno attivo, anche attraverso i media digitali e i social network.
- Favorire una presa di parola consapevole e costruttiva da parte degli alunni diretta a orientare percorsi di peer education.

Nei vari ordini di scuola, l'Istituto Comprensivo, in termini preventivi universali, favorisce la realizzazione di progetti d'Istituto ma anche iniziative che coinvolgono singoli plessi, gruppi di classi, o singole classi, nella progettazione di:

- Percorsi di educazione socio-affettiva ed emotiva;
- Laboratori centrati sul riconoscimento e la gestione delle emozioni;
- Progetti di educazione all'ascolto e alla cura;
- Percorsi progressivi per lo sviluppo delle competenze di empatia e accoglienza dell'altro;
- Iniziative di solidarietà accompagnate da eventi formativi e di animazione socioculturale (Save the cildren – Unicef – Emergency – progetto La Scuolina …);
- Cura di azioni didattico-formative con ricadute indirette (Shoah e Giornata della Memoria, Giornata del Ricordo …)

Nel caso di rilevazione di fenomeni degenerativi di cyberbullismo come l'hate speech, si provvederà ad avviare i protocolli indicati nelle procedure interne segnalate al Cap. 5.

4.4 - Dipendenza da Internet e gioco online

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

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

La dipendenza da Internet è stata definita dallo psichiatra Ivan Goldberg nel 1996 I.A.D. "Internet Addiction Disorder" come "un vero e proprio abuso della tecnologia". Esso presenta tipiche manifestazioni di: dominanza del pensiero; alterazioni del tono dell'umore; conflitti inter e intra-personali da dipendenza; ricaduta e tendenza a ricominciare (Sindrome di Hikikomori). Alcune manifestazioni psico-fisiche tipiche sono: la tolleranza e l'astinenza; l'ansia; l'agitazione psicomotoria; le fantasie; i pensieri ossessivi …. 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. Per quanto riguarda il gioco virtuale l'OSM (osservatorio mondiale della sanità) ha inserito, all'interno del Manuale Diagnostico Statistico dei Disturbi Mentali (DSM 5), la dipendenza dal gioco online. Esso si realizza quando c'è un abuso, ossia un utilizzo continuativo e sistematico della Rete al fine di giocare impegnando la maggior parte della giornata, con la conseguente sottrazione del tempo alle altre attività quotidiane del minore.

Il nostro Istituto presta particolare attenzione ai segnali comportamentali degli studenti da cui si può evincere un attaccamento morboso al gioco online o all'abuso di navigazione virtuale; i docenti che rilevano tali tendenze, attivano percorsi finalizzati alla rieducazione all'uso del digitale, anche in forma ludica, per mediare conoscenze o per stimolare la partecipazione dei ragazzi in progetti di ampio respiro come quelli integrati su eTwinning o le linee programmatiche previste con i Progetti Europei.

Nel caso dei più piccoli, in cui risulta ancor più semplice rilevare le dirette conseguenze dell'uso eccessivo dei videogiochi e del web, la scuola attiva una serie di iniziative alternative che non demonizzano l'uso del gioco online ma lo indirizzano e declinano alla didattica offrendo inoltre ai bambini strumenti critici e di autoregolazione che permettono di prevenire futuri casi di dipendenza (attività di: presentazione di case studies; ascolto dinamico dei segnali d'allarme; lettura autonoma del PEGI e della segnaletica dei videogiochi per l'infanzia e l'adolescenza…). Inoltre il nostro Istituto Comprensivo favorisce percorsi che mirano al controllo della tecnologia, al benessere e all'utilizzo del suo pieno potenziale per trarne vantaggi culturali, sociali e di sana relazione. Tali

percorsi vengono svolti proponendo valide alternative metodologiche e didattiche con l'utilizzo di giochi virtuali d'aula e l'uso del web orientato da obiettivi di natura sempre concreta, socio-relazionale e formativa.

4.5 - Sexting

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

Il Sexting (abbreviazione di sex e texting) indica l'invio e/o la ricezione di contenuti foto/video sessualmente espliciti che ritraggono se stessi o gli altri. Tali contenuti vengono prodotti e trasmessi con l'uso degli smartphone arrivando a creare seri problemi, sia personali che legali, alla persona ritratta. L'invio di foto che ritraggono minorenni al di sotto dei 18 anni in pose sessualmente esplicite configura il reato di distribuzione di materiale pedopornografico. Inoltre i contenuti sessualmente espliciti possono diventare materiale di ricatto assumendo la forma di "revenge porn", con diffusione illecita e incontrollata di immagini o di video sessualmente espliciti. Il fenomeno si caratterizza per: la fiducia tradita; la pervasività con cui si diffondono i contenuti; la persistenza del fenomeno alla rimozione. Tutto ciò finisce per danneggiare inevitabilmente i ragazzi e le ragazze coinvolti, sia in termini psicologici che sociali, oltre che legali, per coloro che hanno contribuito a diffonderla. I rischi correlati del sexting, legati al revenge porn, possono contemplare: violenza psicosessuale, umiliazione, bullismo, cyberbullismo, molestie, stress emotivo, ansia diffusa, sfiducia e depressione.

Nel nostro Istituto Comprensivo, considerata l'età delle utenze, si profila la necessità di attivare azioni di prevenzione universale attraverso l'inserimento nel curricolo di temi legati all'affettività, alla sessualità e alle differenze di genere, nonché iniziative come quelle già descritte al paragrafo 4.1. "Sensibilizzazione e Prevenzione".

Qualora si pervenisse alla rilevazione di casi in cui vi è stata trasmissione di immagini compromettenti si provvederà alla convocazione dei genitori e all'attivazione di specifici percorsi di rieducazione all'uso adeguato del digitale e del web, se necessario anche con il supporto di figure esperte. Si richiamerà la famiglia ricordando loro che l'invio e la detenzione di foto che ritraggono minorenni in pose sessualmente esplicite configura il reato di distribuzione di materiale pedopornografico. Si suggerirà, inoltre, l'attivazione di adeguate forme di controllo parentale della navigazione.

Gli allievi dell'Istituto, soprattutto le classi terze della Scuola secondaria di I grado, verranno adeguatamente coinvolti in percorsi di sviluppo della consapevolezza sugli esiti nefasti di determinati comportamenti attuati con l'uso inconsapevole dei device e del web. Verranno perciò

proposti, soprattutto in occasione del "Safer Internet Day" e del mese della prevenzione all'uso sicuro e responsabile del web, percorsi volti a far comprendere come una foto o un video possano diffondersi in maniera virale in rete divenendo di pubblico dominio in maniera incontrollabile e irrimediabilmente devastante. Alcuni percorsi, già sperimentati in alcune classi, prevedono l'uso dei materiali offerti e disseminati da Generazioniconnesse e Piattaformaelisa, oltre al supporto di esperti.

Nei casi di rilevante gravità si provvederà ad informare tempestivamente il Dirigente Scolastico e attivare i protocolli seguendo le procedure interne segnalate al Cap. 5.

4.6 - Adescamento online

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

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

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

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

Bambini e bambine, ragazzi e ragazze, possono essere potenziali vittime dell'adescamento online poiché il fenomeno non conosce distinzione di genere. Gli adolescenti inoltre risultano particolarmente vulnerabili, essendo importanti fruitori del digitale impegnati nella fragile costruzione evolutiva dell'identità sessuale. Talvolta essi, attratti da relazioni intime e apparentemente rassicuranti, sentono il bisogno di avere attenzioni esclusive da un'altra persona e di ottenere rinforzi esterni d'approvazione. In tal modo finiscono nelle maglie dell'adescamento online, che non avviene apparentemente con una dinamica violenta, ma con il malcelato "prendersi cura". Spesso può capitare che l'adescatore si presenti al minore sotto falsa identità, fingendo quindi di essere un'altra persona così da attirare maggiormente l'attenzione del minore, talvolta si finge coetaneo. I luoghi virtuali in cui prendono forma più frequentemente tali dinamiche sono i canali digitali privilegiati da bambini e adolescenti, le chat, soprattutto quelle dei giochi online, e i

social network frequentati da adolescenti .

Il processo di adescamento segue generalmente 5 fasi:

1. Fase dell'amicizia iniziale
2. Fase del rapporto dialogico privato
3. Fase della costruzione del rapporto di fiducia
4. Fase dell'esclusività
5. Fase della relazione sessualizzata

Per identificare e riconoscere un eventuale caso di adescamento online è importante prestare attenzione a piccoli segnali che possono essere indicatori importanti, come ad esempio un cambiamento improvviso nel comportamento di un minore. Alcuni segnali a cui prestare particolare attenzione riguardano la presenza di:

- Conoscenze sessuali non adeguate all'età del minore;
- Diffusione di video o foto compromettenti che circolano online o che il minore ha ricevuto o filmato;
- Eccessiva attenzione e premura per una relazione online intrattenuta da un adolescente;
- Rilevazione o percezione di allusioni sessuali o prese in giro particolari destinate dai pari nei confronti di un/a bambino/a ragazzo/a.

La problematica dell'adescamento online, come quella del sexting, quindi, si inquadra in uno scenario più ampio di scarsa educazione emotiva, sessuale e di assenza di competenza digitale. Per questo il nostro Istituto ritiene fondamentale portare avanti, soprattutto nelle classi della scuola secondaria di I grado, in termini preventivi universali, progetti e iniziative che coinvolgono singoli plessi, gruppi di classi, o singole classi, in:

- Percorsi di educazione socio-affettiva ed emotiva;
- Laboratori centrati sull'autostima, il riconoscimento e la gestione delle emozioni;
- Progetti di educazione sessuale e sull'identità di genere;
- Percorsi di educazione digitale che includano competenze inerenti: la protezione della propria privacy; la gestione dell'immagine e dell'identità online; la capacità di gestire responsabilmente le proprie relazioni online; lo sviluppo della consapevolezza dell'assunzione da parte di terzi di identità finalizzate all'adescamento.

Se si sospetta o si ha la certezza di un caso di adescamento online è importante: avviare gli specifici protocolli seguendo le procedure interne segnalate al Cap. 5; orientare la cura delle prove e tracce dell'adescamento per la loro non compromissione; richiedere l'intervento immediato della Polizia Postale e delle Comunicazioni; coinvolgere un Servizio territoriale (Consultorio Familiare, Servizio di Neuropsichiatria Infantile ...) in grado di fornire alla vittima anche un adeguato supporto di tipo psicologico o psichiatrico; richiedere eventuale supporto e orientamento Helpline di Generazioni Connesse (1.96.96)

4.7 - Pedopornografia

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

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

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

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

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

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

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

Il tema della pedopornografia è estremamente delicato e nel nostro Istituto Comprensivo risulta opportuno correlarlo strategicamente in un'ottica di attività preventive. Occorre che se parli in considerazione della maturità e della fascia d'età, selezionando con attenzione il tipo di informazioni da condividere. Non risulta assolutamente utile diffondere tra bambini e bambine la conoscenza e l'uso di servizi come le hotline con il rischio di incentivare la ricerca proattiva, che comunque è

vietata dalla legge italiana, per minori e per adulti. Risulta invece utile e opportuna l'attività educativa centrata sui temi dell'affettività e delle relazioni, sottolineando sempre la necessità di rivolgersi ad un adulto ogni qualvolta si incontrino online contenuti che mettono a disagio.

La pedopornografia è tuttavia un fenomeno di cui il mondo adulto deve avere ampia consapevolezza e di cui è utile parlare soprattutto in vista di fenomeni correlati, sempre più frequenti nel mondo adolescenziale, come quelli di sexting e cyberbullismo.

L'Istituto Comnprensivo Sanluri, in tal senso, si occupa di formare/informare e sensibilizzare docenti e famiglie attraverso la promozione dei servizi delle hotline tramite i percorsi di formazione e aggiornamento promossi da www.generazioniconnesse.it ma anche attraverso la programmazione periodica di attività formative dedicate così come riferite al paragrafo 4.1. "Sensibilizzazione e prevenzione".

L'immersione nelle nuove tecnologie dei nativi digitali comporta spesso l'inconsapevolezza rispetto al fatto che una foto o un video diffusi in rete potrebbero non essere mai più estinguibili o, ancora, l'inconsapevolezza che scambiare o diffondere materiale che viene catalogato come pedopornografico rappresenti un reato. Nei casi di detenzione e fruizione di materiali compromettenti, se l'entità è lieve occorre in primo luogo parlarne con alunne e alunni e rispettive famiglie, ricordando loro che l'invio e la detenzione di foto che ritraggono minorenni in pose sessualmente esplicite configura il reato di distribuzione di materiale pedopornografico; in casi di rilevante gravità occorre informare tempestivamente il Dirigente Scolastico e avviare i protocolli e gli adempimenti seguendo le procedure interne segnalate al Cap. 5 del presente documento di e-policy.

Il nostro piano d'azioni

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

- Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse.
- Organizzare uno o più incontri di formazione all'utilizzo sicuro e consapevole di Internet e delle tecnologie digitali integrando lo svolgimento della didattica e assicurando la partecipazione attiva degli studenti/studentesse.
- Organizzare uno o più incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/lle studenti/studentesse.
- Organizzare laboratori di educazione socio-affettiva ed emotiva, rivolti agli/lle studenti/studentesse.

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

- Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse.
- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti agli/lle studenti/studentesse, con il coinvolgimento di esperti.
- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti.
- Organizzare uno o più incontri di formazione all'utilizzo sicuro e consapevole di Internet e delle tecnologie digitali integrando lo svolgimento della didattica e assicurando la partecipazione attiva degli studenti/studentesse.
- Promuovere incontri e laboratori per studenti e studentesse dedicati all'Educazione Civica Digitale.
- Organizzare uno o più incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/lle studenti/studentesse.
- Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/lle studenti/studentesse.
- Pianificare e realizzare progetti di peer-education sui temi della sicurezza online nella scuola.

Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

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

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

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

Nelle procedure:

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

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

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

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

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

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

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

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

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

Vi suggeriamo, inoltre, i seguenti servizi:

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

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

I docenti e il personale della scuola, sono chiamati a rilevare le situazioni di criticità degne di nota, rivolgersi al Dirigente Scolastico o ai Referenti per la prevenzione e il contrasto del bullismo e cyberbullismo che si occuperanno, valutato il caso, di avviare le rispettive procedure. Tali rilevazioni e segnalazioni devono avvenire secondo i protocolli e le disposizioni operate da

“Generazioniconnesse” seguendo la traccia e gli schemi di sintesi allegati, destinati alle diverse situazioni di emergenza richiamate. I docenti avranno anche a disposizione uno strumento di rilevamento delle criticità (di cui si allega copia), sul quale saranno tenuti a descrivere le situazioni che si vengono a determinare, indicando anche le azioni messe in atto; eventualmente è prevista l’integrazione di informazioni con l’uso di un “diario di bordo” sotto forma di Schema riepilogativo delle situazioni gestite (di cui si allega copia).

Si considerano da segnalare tutte quelle situazioni caratterizzate da volontarie e ripetute aggressioni mirate a insultare, minacciare, diffamare e ferire una persona, o un gruppo, tramite l’uso irresponsabile del web. La scuola avrà cura di porre attenzione alla rilevazione di rischi connessi alla navigazione sul web e alle correlate attività di sensibilizzazione e prevenzione. In modo particolare l’Istituto dovrà rilevare e monitorare sistematicamente le problematiche connesse al cyberbullismo, all'adescamento online e al sexting.

In particolare saranno elementi di urgente segnalazione:

- Contenuti afferenti la violazione della privacy (foto personali; indirizzo di casa; recapito telefonico; informazioni private proprie o di amici; foto o video pubblicati contro la propria volontà…);
- Contenuti afferenti all’aggressività o alla violenza (messaggi minacciosi; commenti offensivi e denigratori; pettegolezzi; informazioni false; foto o video imbarazzanti; virus; contenuti razzisti; contenuti di inneggio al suicidio; immagini o video umilianti; insulti; videogiochi pensati per un pubblico adulto …);
- Contenuti afferenti alla sessualità (messaggi molesti e sessualmente connotati; conversazioni che richiamano relazioni intime e sessualizzate; produzione, detenzione e diffusione di foto e video personali con nudità, immagini pornografiche; produzione, detenzione e diffusione di foto e video in cui persone di minore età sono coinvolte o assistono ad attività sessuali, pedopornografia …)

Nelle procedure:

- Si farà riferimento alle figure preposte all’accoglienza della segnalazione e alla presa in carico e gestione del caso;
- Si procederà all’immediato coinvolgimento del Dirigente Scolastico e dei Referenti per il contrasto del bullismo e del cyberbullismo;
- Si passerà alla gestione del caso con la presa in carico da parte del Team preposto alla gestione interna della segnalazione e/o all’invio ai soggetti esterni preposti competenti.

Gli insegnanti, in quanto incaricati di pubblico servizio, hanno l’obbligo di comunicare al Dirigente Scolastico e di denunciare i reati perseguibili d’ufficio di cui vengano a conoscenza, l’elenco dei reati è rinviato alla scheda allegata.

Per quanto riguarda la segnalazione finalizzata alla rimozione di contenuti online lesivi si allega il modello semplificato da indirizzare al Garante per la protezione dei dati personali, ad uso del minore ultraquattordicenne che sia stato vittima di cyberbullismo, o dei suoi genitori, e finalizzato alla rimozione o al blocco dei contenuti diffusi nel web .

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.

I DOCENTI, IL PERSONALE DELLA SCUOLA E I GENITORI

La comunità educante e in particolar modo i docenti, si occupano di rilevare possibili situazioni di disagio connessi a uno o più dei rischi riferiti, attraverso la segnalazione al Dirigente Scolastico e ai Referenti per il Bullismo e Cyberbullismo, compilando il modulo per la segnalazione dei casi (Allegato).

Sulla base del livello di problematicità rilevato, il caso verrà trattato con differenti approcci, strumenti e metodi attivando i protocolli di prevenzione (universale, selettiva o indicata) maggiormente consoni alla situazione così come riferiti al Cap. 4.1.

- I casi a bassa problematicità saranno gestiti dal Team dei docenti guidati dal coordinatore di classe con il supporto tecnico dei Referenti per la prevenzione e il contrasto del bullismo e cyberbullismo;
- I casi di media problematicità saranno gestiti dal Team dei docenti guidati dal coordinatore di classe con il supporto tecnico dei Referenti per la prevenzione e il contrasto del bullismo e cyberbullismo; in tal caso sarà informato il Dirigente Scolastico, verrà coinvolta la famiglia e ci si appoggerà alle consulenze dello psicologo della scuola, quando disponibile, e/o ai servizi socio-sanitari territoriali.
- I casi di rilevante problematicità saranno trattati con i protocolli formali che prevedono in prima istanza l'urgente segnalazione al Dirigente Scolastico e ai Referenti Bullismo e Cyberbullismo, i quali si attiveranno per l'avvio delle procedure come indicate negli schemi allegati.

GLI ALUNNI

Gli alunni potranno segnalare possibili situazioni problematiche o di disagio che stanno vivendo in prima persona, o di cui sono testimoni, sia attraverso le consuete comunicazioni confidenziali con i docenti di classe, che attraverso alcuni strumenti di cui si darà adeguata comunicazione e pubblicizzazione. In particolare si prevede la fornitura di:

- Indirizzo su piattaforma microsoft 365 education dei Referenti per la prevenzione e il contrasto del bullismo e cyberbullismo, finalizzati alla trasmissione di messaggi personali di segnalazione;
- Scatola/box per la raccolta di segnalazioni anonime, da inserire in uno spazio accessibile e ben visibile nella Scuola Secondaria di I grado;
- Sportello di ascolto con professionisti psicologi/pedagogisti/educatori, di volta in volta disponibili sulla base di specifici percorsi e progetti;
- Periodiche rilevazioni del benessere attraverso la compilazione di questionari strutturati indirizzati ai bambini e ai ragazzi, finalizzati anche alla trasmissione e raccolta di istanze personali.

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.

Di seguito vengono riportati i contatti dei servizi territoriali di riferimento cui rivolgersi per la gestione degli eventuali casi di rilevante problematicità:

UNICEF SARDEGNA

Indirizzo: Presso Comando Provinciale VV.F. Viale Marconi, 300 - 09131 Cagliari
Recapito telefonico: 328 55 39 921

Mail: comitato.sardegna@unicef.it

Sito: www.unicef.it

CORECOM

Indirizzo: Via Roma, 25 - 09125 Cagliari

Recapito telefonico: 070 668685

Mail: corecom@consregsardegna.it

Sito: www.consregsardegna.it

USR SARDEGNA

Indirizzo: V.le Regina Margherita n. 6 - 09125 Cagliari

Recapito telefonico: 070 65004252-78

Mail: direzione-sardegna@istruzione.it

Sito: www.usrsardegna.it

POLIZIA POSTALE E DELLE COMUNICAZIONI

Indirizzo: Via Simeto, 38 - 09131 Cagliari

Recapito telefonico: 070 27665

Mail: poltel.ca@poliziadistato.it

Sito: www.commissariatodips.it

GARANTE REGIONALE PER L'INFANZIA E L'ADOLESCENZA

Indirizzo: Via Roma 25 - 09125 Cagliari

Recapito telefonico: 070. 6014332

Mail: garanteinfanzia@conregsardegna.it garanteinfanzia@pec.crsardegna.it

Sito: www.consregsardegna.it

TRIBUNALE PER I MINORI DI CAGLIARI

Indirizzo: Via Dante - 09128 Cagliari

Recapito telefonico: 070 34921 fax 070 307600

Mail: tribmin.cagliari@giustizia.it

Sito: www.giustizia.sardegna.it

ASSL SANLURI

Indirizzo: Via Giuseppe Ungaretti, 9 - 09025 Sanluri (SU)

Recapito telefonico: 070 93841 fax 070 9384311 -070 9359457 -070 9359440

Struttura Ufficio: Neuropsichiatria dell'età evolutiva - via Bologna 13

Sito: www.aslsanluri.it

COMUNE DI SANLURI Servizi Sociali e alla Persona

Indirizzo: Via Alberto Riva Villasanta, 17 - 09025 Sanluri

Recapito telefonico: 070 9301709

Mail: serviziosociale@comune.sanluri.su.it

Sito: www.comune.sanluri.su.it

www.generazioniconnesse.it

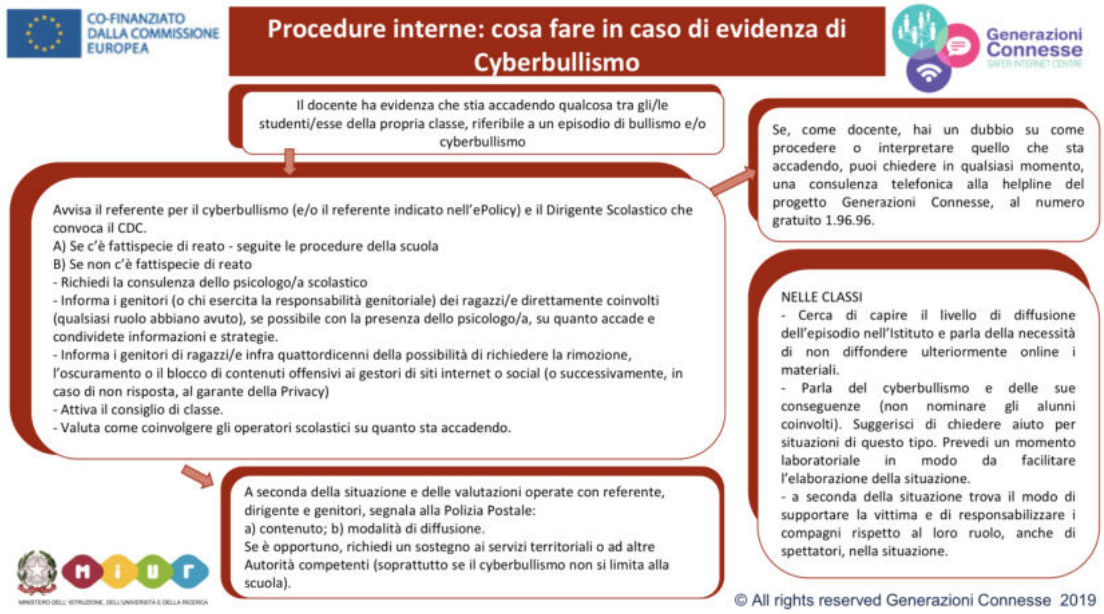
Telefono Azzurro: Help line 1.96.96

Telefono Azzurro: www.azzurro.it/it/clicca-e-segnala

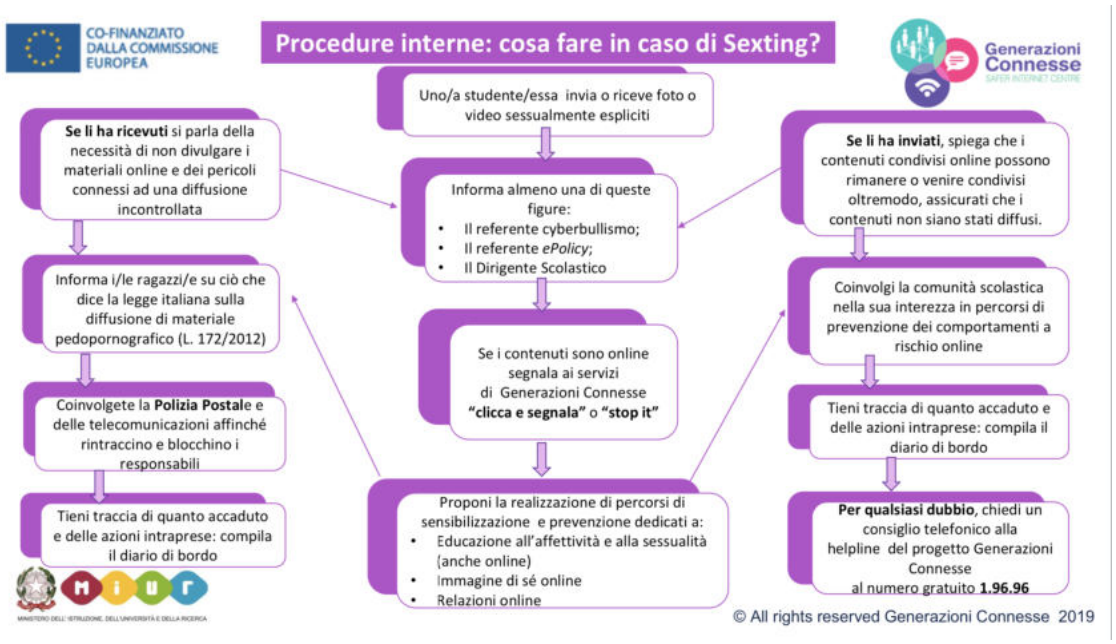
Save the Children: www.stop-it.it/

5.4. - Allegati con le procedure

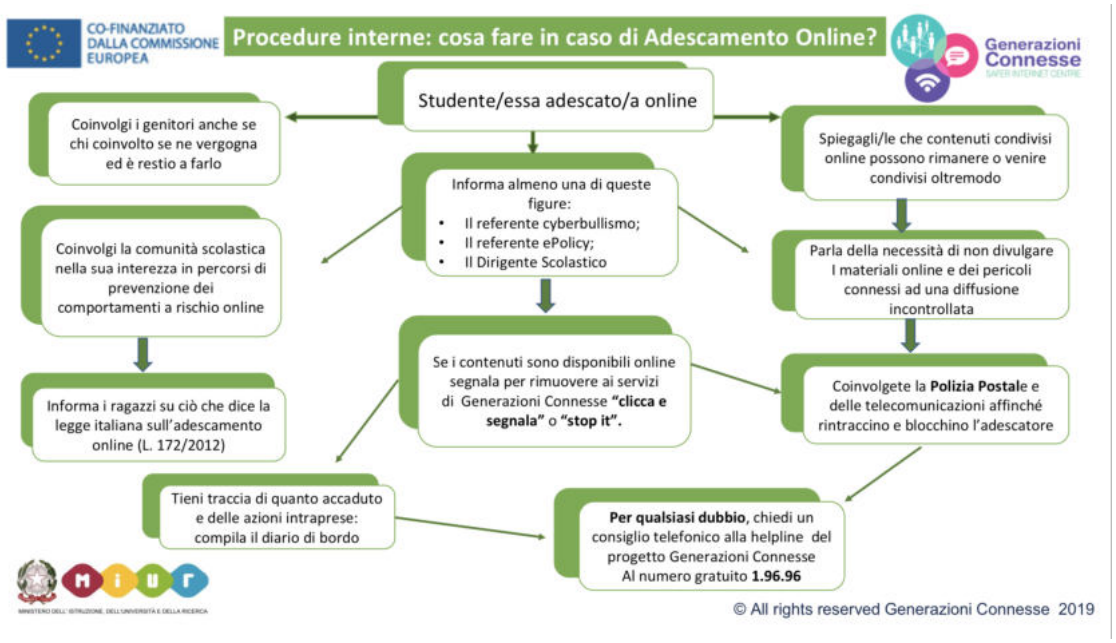
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



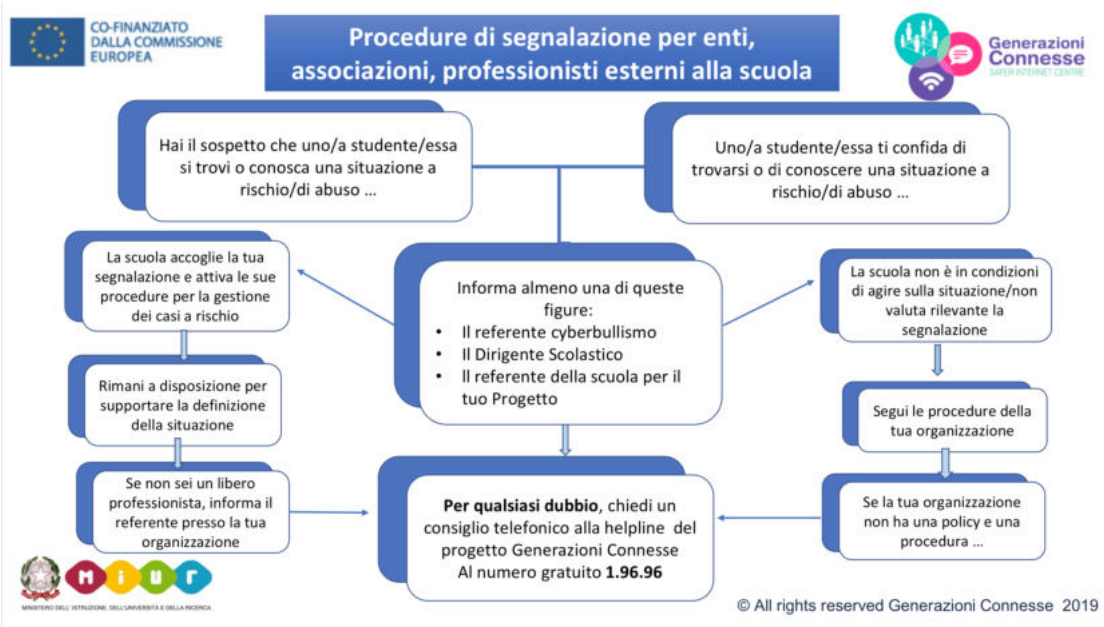
Procedure interne: cosa fare in caso di sexting?



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

La procedura da seguire una volta che è stato rilevato un presunto episodio di bullismo o cyberbullismo con conseguente vittimizzazione, prevede sinteticamente quattro fasi:

1. **La segnalazione**, grazie alla quale si attiva un processo di attenzione e di successive valutazioni relative ad un presunto caso di bullismo o cyberbullismo, che conduce al processo di presa in carico dopo aver escluso l'eventuale erronea analisi interpretativa della situazione di prepotenza. La segnalazione può essere espressa da uno dei soggetti della Comunità Educante, in genere il docente, oppure da uno studente dell'Istituto attraverso l'uso dei canali e degli strumenti messi a disposizione. L'episodio viene poi segnalato al Dirigente Scolastico e ai Referenti Bullismo e Cyberbullismo.
2. **La valutazione e l'approfondimento** vengono attivati con tutti gli attori coinvolti, previa compilazione del modulo per le segnalazioni cui fa seguito una fase di approfondimento del caso a cura del Team Antibullismo. Il Team è composto da: il Dirigente Scolastico; i due Referenti Bullismo; l'Animatore Digitale; il Coordinatore di classe e il Referente del plesso in cui è stato rilevato e segnalato il caso. Il Team Antibullismo è preposto alla gestione interna della segnalazione e/o all'eventuale invio ai soggetti esterni competenti.

3. **La scelta dell'intervento e la gestione del caso** viene svolta o internamente dal Team, attraverso l'identificazione delle misure educative e degli interventi disciplinari da comminare al bullo/cyberbullo con la rapida scelta delle misure di riduzione e contenimento del danno subito dalla vittima, oppure viene affidata per la parte di competenza alle autorità esterne. Tra gli interventi educativi si riferiscono a titolo esemplificativo ma non esaustivo: Incontri tematici con gli alunni coinvolti; Interventi di discussione e confronto in classe; Percorsi laboratoriali e di sensibilizzazione; Attività formativo/informative rivolta ai genitori; Responsabilizzazione degli alunni coinvolti; Percorsi di rivisitazione e condivisione delle regole di classe; Counselling a sportello ecc. Tra le misure disciplinari da comminare al bullo/cyberbullo si riferiscono a titolo esemplificativo ma non esaustivo: Il richiamo verbale; Il richiamo verbale con particolari conseguenze (riduzione o sospensione di attività gratificanti); Il richiamo scritto con annotazione sul diario e sul registro elettronico; La convocazione dei genitori da parte degli insegnanti; La convocazione dei genitori da parte del Dirigente Scolastico; La formulazione di scuse ufficiali e incontri chiarificatori di riparo e risoluzione con la vittima; Compiti relativi al bullismo; Attività e compiti a favore dell'intera comunità scolastica; Percorsi rieducativi anche con la collaborazione di Enti esterni...
4. **Monitoraggio** sistematico del caso a cura del Team e, se necessario, con l'eventuale supporto di esperti, anche a seguito della completa risoluzione delle problematiche connesse agli episodi segnalati. Il monitoraggio prevede la definizione e implementazione di attività di supervisione e accompagnamento rivolte sia al bullo che alla vittima. L'eventuale rimodulazione delle azioni di intervento e gestione del caso viene contemplata qualora gli interventi e le misure portate avanti non avessero sortito gli esiti attesi.

Il nostro piano d'azioni

Non è prevista nessuna azione.