



Documento di ePolicy

SSIC813003

"ANTONIO GRAMSCI" - OSSI

VIA EUROPA - 07045 - OSSI - SASSARI (SS)

MARCELLA Fiori

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 curriculum**
 1. Curriculum 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.

L'Istituto Comprensivo "A.Gramsci" si dota di una e-policy, progetto Web Sicuro, avente come finalità quella di sensibilizzare studenti e studentesse, genitori ed insegnanti su un uso corretto consapevole e responsabile della Rete sì da coglierne tutte le opportunità con la massima sicurezza.

Come evidenziato nelle linee d'indirizzo della DS, nella nostra Scuola si ha particolare attenzione allo sviluppo e potenziamento delle competenze digitali degli insegnanti e degli studenti, anche con l'adozione di una didattica digitale integrata, all'insegna della creatività, dello sviluppo e valorizzazione dei talenti di ognuno.

Nel contempo si impegna nella prevenzione e contrasto della dispersione scolastica, di ogni forma di discriminazione e del bullismo, anche informatico, con formazione e implementazione di protocolli di attenzione e reazione ai fenomeni correlati.

Del resto, le attività di promozione all'utilizzo delle tecnologie digitali nella didattica costituiscono un tema centrale per l'attuazione del Piano Nazionale Scuola Digitale a cui l'I.C Gramsci aderisce e sono già previste nel Piano Triennale dell'Offerta Formativa.

Tale documento programmatico, in riferimento alle tecnologie digitali, delinea sia la proposta formativa che la vision che la sottende. L'e policy è redatto nell'ambito dell'iniziativa Generazioni connesse. Oggi, il progetto Generazioni Connesse, oltre a godere del patrocinio della Commissione Europea e del Miur, è realizzato in partenariato con le principali realtà nazionali che si occupano di sicurezza in Rete.

Viene inserito nel Piano Triennale dell'Offerta Formativa e le azioni preventivate nel Piano d'Azione della nostra scuola verranno portate avanti progressivamente nel prossimo triennio; altresì è elemento unificante di vari regolamenti già in essere.

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.

La Dirigente Scolastica, prof.ssa Marcella Fiori

La Dirigente Scolastica garantisce la sicurezza, anche online, di tutti i membri della comunità scolastica. E' formata adeguatamente sulla sicurezza e sulla prevenzione di problematiche offline e online, in linea con il quadro normativo di riferimento e le indicazioni del MIUR; promuove la cultura della sicurezza online e dà il proprio contributo all'organizzazione, insieme ai docenti referenti della formazione e del bullismo/cyberbullismo, di corsi di formazione specifici per tutte le figure scolastiche sull' utilizzo positivo e responsabile delle TIC. Sollecita l'uso tecnologie didattiche innovative. Sensibilizza e coinvolge studenti, docenti e genitori, con progetti e percorsi formativi ad hoc. Gestisce ed interviene nei casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali.

L'Animatore digitale, supportato dal Team Digitale, ins. Salvatore Faedda

L'Animatore digitale supporta il personale scolastico da un punto di vista non solo tecnico-informatico, ma anche in riferimento ai rischi online, alla protezione e gestione dei dati personali, oltre che essere uno dei promotori di percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale" (con riferimento, ad esempio, allo sviluppo delle competenze digitali previste nelle classi SMART e nell'ambito dell'educazione civica); coordina e gestisce la piattaforma Moodle e G-Suite D'istituto e assiste docenti, genitori e alunni nel loro utilizzo; monitora e rileva eventuali episodi o problematiche connesse all'uso delle TIC a scuola e ha il compito di controllare che la Rete della scuola sia sicura.

La Referente bullismo e cyberbullismo, prof.ssa Simonetta M. Schintu, supportata dal Team antibullismo proff. Maria Franca Campus, Salvatore Faedda, Gabriella Farina e Anna Marongiu.

Coordina e promuove iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo. Raccoglie e diffonde documentazione e buone pratiche; Crea sul sito istituzionale un'apposita sezione. Progetta attività specifiche di orientamento, formazione - prevenzione per docenti e alunni; Valorizza metodologie innovative; Coinvolge gli studenti per progettare percorsi formativi rispondenti ai loro bisogni (uso consapevole dei social network, rischi presenti nella rete...); Crea una sezione sul sito istituzionale che rimanda a: www.generazioniconnesse.it, sito del MIUR, per informazioni di carattere generale; Sensibilizza e coinvolge studenti, colleghi e genitori con progetti e percorsi formativi; può avvalersi della collaborazione delle Forze di polizia, delle associazioni e dei centri di aggregazione giovanile del territorio.

I Referenti del sito web, proff. Mario Pittalis e Pierangela Lubinu

Si occupano della manutenzione e aggiornamento della struttura del sito web dell'Istituto Comprensivo secondo quanto previsto dalla normativa vigente, con particolare attenzione agli aspetti legati alla privacy e alla trasparenza; aggiornano costantemente il sito con inserimento di documenti previsti dalla normativa vigente e materiali vari, sottoposti, in via preventiva, all'attenzione della Dirigente Scolastica per la necessaria autorizzazione; collaborano con il personale di Segreteria incaricato della pubblicazione dei provvedimenti di competenza nelle sezioni Albo on line e Amministrazione Trasparente; acquisiscono informazioni e materiali dai docenti referenti dei progetti didattici al fine della loro pubblicazioni; curano la progettualità relativa al settore di competenza..

I Docenti

Tutti i docenti diffondono la cultura dell'uso responsabile delle TIC e della Rete. Aderiscono e diffondono l'ePolicy. Integrano parti del curriculum della propria disciplina con approfondimenti ad hoc, promuovendo l'uso delle tecnologie digitali nella didattica. I docenti accompagnano e supportano gli studenti e le studentesse nelle attività di apprendimento e nei laboratori che prevedono l'uso di dispositivi che si connettono alla Rete; promuovono una cultura dell'uso responsabile delle TIC e della rete, guidano gli studenti e le studentesse a distinguere siti e notizie affidabili, usano e fanno usare in maniera corretta i sistemi informatici, responsabilizzano a rispettare il diritto d'autore e dal diffondere dati personali; segnalano alla Dirigente Scolastica qualunque problematica, violazione o abuso, anche online, che vede coinvolti studenti e studentesse.

La Direttrice dei Servizi Generali e Amministrativi, rag. Giuseppa Martinez

Amministra le password ed assicura la riservatezza dei dati personali trattati ai sensi della normativa vigente; garantisce il funzionamento dei diversi canali di comunicazione della scuola all'interno della scuola e fra la scuola e le famiglie degli alunni per la notifica di documenti e informazioni della Dirigente scolastica e dell'Animatore digitale nell'ambito dell'utilizzo delle tecnologie digitali e di internet; assicura, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per garantire che le apparecchiature multimediali dei plessi scolastici siano funzionanti e sicure.

Il personale Amministrativo, Tecnico e Ausiliario (ATA)

Il personale ATA segnala comportamenti non adeguati riguardanti l'uso di device e/o episodi di bullismo/cyber bullismo.

Gli Studenti e le Studentesse

Gli Studenti e le Studentesse utilizzano al meglio le tecnologie digitali in coerenza con quanto richiesto dai docenti; con il supporto della scuola imparano a tutelarsi online, tutelare i/le propri/e compagni/e e rispettarli/le; partecipano attivamente a progetti ed attività che riguardano l'uso positivo delle TIC e della Rete e si fanno promotori di quanto appreso anche attraverso possibili percorsi di peer education; rispettano gli strumenti della scuola, compresi gli ipad in comodato, senza alterarne condizioni e configurazioni

I Genitori

I Genitori, in continuità con l'Istituto scolastico, sono partecipi e attivi nelle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete, nonché sull'uso responsabile dei device personali; si relazionano in modo costruttivo con i docenti sulle linee educative che riguardano le TIC e la Rete, concordano linee comuni d'intervento e comunicano con loro circa i problemi rilevati quando i/le propri/e figli/e non usano responsabilmente le tecnologie digitali o Internet. Poichè esiste una corresponsabilità educativa e formativa che riguarda sia i genitori che la scuola nel percorso di crescita degli studenti e delle studentesse, accettano e condividono quanto scritto nell'ePolicy dell'Istituto.

Gli Enti educativi esterni e le associazioni

Gli Enti educativi esterni e le associazioni che entrano in relazione con la scuola si conformano alla politica della stessa riguardo all'uso consapevole della Rete e delle TIC; promuovono comportamenti sicuri, la sicurezza online e assicurano la protezione degli studenti e delle studentesse durante le attività che si svolgono insieme.

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).

L'Istituto Comprensivo "A.Gramsci" OSSI pubblica il documento di ePolicy, nel sito della scuola (<https://www.icantoniogramscioggi.edu.it/>), in home page, dove è liberamente consultabile.

Le figure professionali e le organizzazioni coinvolte in progetti, laboratori e attività prenderanno visione e sottoscriveranno un'informativa (MODULO ALLEGATO) che lo attesti, preliminarmente all'avvio dei programmi con gli studenti e le studentesse, in classe o fuori. L'Istituto potrebbe anche richiedere, eventualmente, il casellario giudiziale e la presenza di un codice di condotta adottato dalla propria organizzazione o associazione (cooperativa, ente di formazione, servizio, etc.), come fattore ulteriormente protettivo verso i minori.

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/le 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.

Nello specifico il documento di e-policy viene condiviso e comunicato:

-agli studenti e alle studentesse: una versione child friendly, discussione in classe nei primi giorni di scuola, con particolare riguardo al protocollo di utilizzo di internet per le nuove classi prime; informazione agli alunni riguardo l'uso responsabile e sicuro di internet ; eventi e dibattiti informativi e formativi, in momenti diversi dell'anno con il coinvolgimento di esperti, sui temi oggetto di questo Documento

al personale scolastico: durante il Collegio Docenti,sul sito e sul registro elettronico con richiesta di presa visione; ai genitori :sul sito istituzionale della scuola, sul registro elettronico con richiesta di presa visione e tramite incontri scuola-famiglia.

Ciascun attore scolastico (dai docenti agli/lle studenti/esse) si fa a sua volta promotore del documento.

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.

Le infrazioni della policy possono essere rilevate dai docenti, dagli ATA, durante l'esercizio delle proprie funzioni, dagli alunni e dai genitori. Particolare attenzione viene richiesta al personale scolastico per le possibili infrazioni nelle quali il personale stesso, soprattutto i docenti, possono incorrere se utilizzano impropriamente i dispositivi o la Rete, nonché in quelle violazioni qualora non intervengano nella segnalazione di condotte improprie dei/lle propri/ie studenti/studentesse.

Per quanto riguarda studenti e studentesse, invece, qualora venga individuata un'infrazione, è necessario informare il coordinatore di classe, il quale a sua volta riferirà alla Dirigente Scolastica e alla famiglia.

Nel caso in cui l'infrazione si configuri come atto di cyberbullismo, il docente informa il referente per il bullismo/cyberbullismo. Nel caso si tratti di un reato è necessario che la Dirigente informi le autorità competenti (polizia postale). Le potenziali infrazioni a carico degli alunni sono identificabili in:

- condivisione online di immagini o video di compagni/e senza il loro consenso o che li ritraggono in pose offensive e denigratorie;
- condivisione di scatti intimi e a sfondo sessuale;
- condivisione di dati personali;
- l'invio di immagini o video volti all'esclusione di compagni/e.
- l'uso improprio di apparecchiature elettroniche o l'accesso a materiali inappropriati;
- l'utilizzo della strumentazione della scuola a scopi personali, ludici e/o ricreativi (a meno che l'attività didattica non lo preveda esplicitamente);
- la modifica della configurazione di sistema delle macchine
- l'utilizzo dei propri dispositivi esterni personali senza aver acquisito il permesso da parte dell'insegnante.

Per ciascuna delle infrazioni all'ePolicy saranno messe in atto azioni educative e/o irrogate sanzioni valutando i diversi gradi di gravità di eventuali violazioni, che vanno dal richiamo verbale dell'insegnante al richiamo scritto della Dirigente scolastica con convocazione della famiglia e allontanamento dalla scuola da uno a tre giorni all'allontanamento dalla scuola per un periodo fra i 3 e i 15 giorni(Così come stabilito dal Regolamento di Disciplina per gli Alunni della Scuola Secondaria contenuto nel nostro Regolamento di Istituto).

<https://www.icantoniogramsciossi.edu.it/index.php/p-o-f/regolamenti-2018-2019>

Nel Capitolo 5 sono esposte le procedure di segnalazione e gestione delle infrazioni (anche in riferimento agli specifici regolamenti in materia).

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.

- Riferimenti all'E-policy sono contenuti nei seguenti allegati del REGOLAMENTO DI ISTITUTO: 1. Regolamento

di disciplina;

<https://www.icantoniogramscioggi.edu.it/index.php/p-o-f/regolamenti-2018-2019>.

2. Protocollo di intervento per la prevenzione e il contrasto dei fenomeni di bullismo e cyberbullismo

<https://www.icantoniogramscioggi.edu.it/attachments/article/173/PROTOCOLLO%20SEGNALAZIONE.pdf>.

3. Regolamento per la DDI

<https://www.icantoniogramscioggi.edu.it/index.php/didattica/didattica-adistanza/614-regolamento-didattica-digitale-integrata-2020-21>.

4.

Regole per l'uso del Cellulare e dei Dispositivi Tecnologici

1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

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

Il monitoraggio sarà curato dalla Dirigente scolastica con la collaborazione della fs area 6 Valutazione e Miglioramento, dell'Animatore digitale, della referente sulla prevenzione del bullismo e cyberbullismo e del gruppo di lavoro (ampliato rispetto a questo a.s.) che predisporrà un questionario proposto a studenti studentesse genitori e docenti in modalità digitale. Sarà finalizzato a rilevare la situazione iniziale delle classi e gli esiti a fine anno, in relazione all'uso sicuro e responsabile delle tecnologie digitali e di internet. Il monitoraggio sarà rivolto anche agli insegnanti, al fine di valutare l'impatto della E-policy e la necessità di eventuali miglioramenti. Sulla base delle risultanze questo documento verrà revisionato ed aggiornato.

Il monitoraggio dell'implementazione della E-policy e del suo eventuale aggiornamento sarà svolta ogni anno.

L'aggiornamento della E-policy sarà curato dalla Dirigente scolastica, dall'Animatore digitale, dalla referente della prevenzione del bullismo e cyberbullismo e dagli Organi Collegiali, a seconda degli aspetti considerati.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

- 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 ai docenti

Azioni da svolgere nei prossimi 3 anni:

- 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 curriculum

2.1. Curriculum 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 curriculum digitale.

Il tema della competenza digitale (digital literacy) è emerso all'interno del dibattito internazionale sul lifelong learning, ovvero sulla definizione dei saperi chiave per vivere attivamente nella cosiddetta Società dell'Informazione, un contesto che richiede un nuovo modello di alfabetizzazione in cui le nuove tecnologie e la rete possono essere considerati veri e propri vettori di partecipazione e la competenza digitale è quindi annoverata tra i saperi necessari per la cittadinanza.

Diventa opportuno pensare la competenza digitale come uno scenario in cui si intersecano dimensioni di natura diversa, che potremmo così schematizzare:

Dimensione tecnologica

Questo ambito fa riferimento a una serie di competenze tecnologiche e digitali come strumenti per la risoluzione di problemi della vita quotidiana, per evitare automatismi che abbiano conseguenze incerte, attraverso

un'adeguata comprensione della "grammatica" dello strumento.

Dimensione cognitiva

Comprende abilità e capacità di cercare, usare e creare in modo critico le informazioni condivise in Rete, valutandone credibilità e affidabilità legate al trattamento dell'informazione, ma anche il saper trattare testi e dati per produrne sintesi, analisi e rappresentazioni con tabelle e grafici;

Dimensione etica e sociale

Questa dimensione riguarda il saper interagire con gli altri in modo corretto e responsabile e comprende alcune delle tematiche più attuali rispetto al tema delle nuove tecnologie, dalla tutela della privacy al contrasto del fenomeno del cyber bullismo.

Dalla integrazione di queste tre principali dimensioni emerge un concetto di competenza digitale che fa riferimento alla capacità di comprendere e sfruttare l'effettivo potenziale delle tecnologie per la costruzione di conoscenze e per la promozione della partecipazione e dell'inclusione: il rapporto con le tecnologie digitali guarda così a forme di uso consapevole, critico e creativo.

Nel nostro Istituto la presenza e l'utilizzo di strumenti tecnologici sono una realtà consolidata da anni, sia come supporto tecnico e compensativo nei casi di disabilità e di disturbi specifici di apprendimento, sia per la possibilità di progettare una didattica che utilizzi linguaggi diversi da quelli propri della lezione frontale, nella consapevolezza che la scuola digitale vada pensata non solo in funzione dell'innovazione fine a se stessa, ma anche e soprattutto delle concrete finalità didattiche. Per tale ragione, è stato elaborato il curriculum secondo il quadro di riferimento e le aree di competenza individuate dal Digcomp 2.1. Il curriculum delle competenze digitali è concepito come un percorso didattico verticale che, nei tre ordini di scuola, permette agli alunni di sviluppare competenze digitali interdisciplinari di facile replicabilità, utilizzo e applicazione.

Per un riscontro si rimanda alla pagina del sito istituzionale relativa al curriculum d'Istituto e alle rubriche di valutazione delle competenze di Educazione Civica <https://www.icantoniogramscirossi.edu.it/index.php/dipartimenti/curricoli-verticali>.

Inoltre, già dall'anno scolastico 2019/20 all'interno dell'offerta formativa si sono programmate unità di apprendimento, progetti ed iniziative varie in verticale, per implementare e rafforzare le abilità, conoscenze e competenze digitali fra tutti gli alunni e le alunne dell'Istituto Comprensivo "A.Gramsci". I percorsi attuati, che hanno messo in evidenza buone pratiche, intendono superare le barriere disciplinari e settoriali e possono essere replicati e riproposti. Alcuni sono già indicati nel PTOF, altri dovranno essere inseriti:

"SETTIMANA DIGITALE"

Nella progettazione delle attività sono coinvolti

tutti gli ambiti disciplinari partendo dalla consapevolezza che ciascuna disciplina può dare il proprio contributo per quanto concerne le attività legate al coding, al pensiero computazionale, alle competenze digitali. A partire dalla scuola dell'infanzia e nei primi due anni della scuola primaria si svolgeranno attività a livello ludico-laboratoriale per la promozione e l'applicazione didattica dei principi base della programmazione per contribuire in modo trasversale e naturale allo sviluppo del pensiero computazionale. Nelle tre classi terminali della scuola primaria le attività precedentemente esposte saranno integrate da quelle legate ad una prima acquisizione della cultura informatica e delle competenze digitali e dallo sviluppo di temi legati alla cittadinanza digitale. Nella scuola secondaria di 1° grado si svolgeranno attività più sistematiche sia nell'uso creativo delle tecnologie sia nel loro utilizzo con spirito critico, legato all'educazione alla cittadinanza digitale, con un'attenta riflessione sulle opportunità e sui rischi a loro connessi. Una valida opportunità sarà offerta dall'eventuale utilizzo della piattaforma Moodle e dalle LIM di cui sono dotate tutte le classi della scuola dell'obbligo. La sperimentazione avviata durante lo scorso anno scolastico pone le basi per un discorso che sarà sviluppato in maniera più sistematica in futuro. Ogni sezione e classe dell'istituto ha la possibilità di sviluppare il percorso ritenuto più idoneo durante la "Settimana digitale" che si svolgerà dal 22 al 28 novembre 2021.

EDUCAZIONE AL PENSIERO COMPUTAZIONALE - CODING

Laboratorio del team digitale per alunni della scuola dell'infanzia e scuola primaria

PRODUZIONE E CONDIVISIONE DI CONTENUTI DIGITALI CON LE APPLICAZIONI MESSE A DISPOSIZIONE DALLA PIATTAFORMA D'ISTITUTO (MOODLE)

EDUCAZIONE ALLA CITTADINANZA DIGITALE: LA COMUNICAZIONE IN RETE

EDUCAZIONE ALLA CITTADINANZA ATTIVA e ALLO SPIRITO DI INIZIATIVA E IMPRENDITORIALITÀ "Creare... nel rispetto delle regole"

LABORATORIO DI INFORMATICA- ALUNNI DSA - Secondaria 1° Grado

TUTORIAL DEL TEAM DIGITALE

destinati a tutti gli alunni e le alunne per acquisire almeno una competenza di base degli strumenti presenti a scuola (hardware e software) nell'utilizzo delle LIM in classe o dei laboratori d'informatica (Qubica 3)

CLASSI SMART

(sperimentazione nelle classi 2[^], della scuola secondaria di Ossi e Tissi) Utilizzo sistematico degli strumenti informatici nella didattica. Incremento delle competenze digitali degli allievi. Riconoscimento di opportunità e rischi delle informazioni e dei contenuti digitali.

Nel perseguire lo sviluppo delle competenze digitali dei propri studenti l'Istituto

comprensivo si ispira al Manifesto della Comunicazione non Ostile, al documento europeo DigComp - 2.1 competenze digitali per la cittadinanza, al decalogo del MIUR, Dieci punti per l'uso dei dispositivi mobili a scuola, ai percorsi di "Generazioni Connesse" e di "Programma il futuro".

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

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

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

La formazione dei docenti e del personale che opera nella scuola è un importante elemento di qualità nel servizio scolastico; essa rappresenta una leva strategica per lo sviluppo culturale dell'istituzione scolastica, per il necessario sostegno agli obiettivi di cambiamento e per un'efficace politica delle risorse umane.

L'attenzione all'uso delle TIC nella didattica rende gli apprendimenti più motivanti, coinvolgenti ed inclusivi, con una funzione di guida da parte del docente; inoltre, permette di sviluppare capacità che sono sempre più importanti anche in ambito lavorativo, come il lavoro di gruppo anche a distanza ed il confronto fra pari in modalità asincrona. La competenza digitale -oggi- è imprescindibile e permette di integrare la didattica con strumenti che la diversificano, la rendono innovativa ed in grado di venire incontro ai diversi stili di apprendimento.

Il Collegio docenti riconosce e favorisce la partecipazione del personale ad iniziative promosse sia direttamente dalla scuola (formazione d'ambito o interna), sia quelle liberamente scelte dai docenti (anche online) purché restino coerenti con il piano di formazione.

L'I.C. "Gramsci" di Ossi è stato nominato, a livello regionale, scuola capofila organizzatrice dei corsi di formazione per l'ambito 001; le

referenti Ins. Pierangela Lubinu e Ins. M. Paola Moro in questi ultimi due anni hanno predisposto differenti attività formative permettendo al gruppo docente di acquisire metodologie e competenze digitali utili per la didattica. Di vasto respiro e discretamente partecipate dai docenti interni hanno riguardato le seguenti tematiche: Tecnologie Didattiche E Ambienti Di Apprendimento Innovativi, Gestione E Creazione Siti Web E Blog Con Wordpress, Dad Gsuite E Microsoft 365, Dad e Valutazione , Dalla Dad (Didattica A Distanza) Alla Ddi (Didattica Digitale Integrata), Flipped Learning Approach, Cittadinanza Digitale, Flipped Learning E Ddi, A Tempo Con La Dad Strumenti A Tempo Con La Dad. Come formazione interna, la nostra scuola, proprio per migliorare le competenze digitali dei docenti anche nella didattica, ha organizzato, con l'aiuto dell'Animatore digitale e di altri esperti interni, vari incontri sull'uso della piattaforma nella DaD. In particolare ha promosso attività sulla piattaforma Moodle, su Google suite for education e su tutte le applicazioni che gravitano intorno ad essa, privilegiando un uso collaborativo di tali strumenti.

Inoltre, i docenti facenti parte i Consigli di classe di 2A Tissi e 2B Ossi hanno frequentato in modalità e-learning, con la guida del formatore Antonello Magaletti ,il Corso Apple Education ,per l'acquisizione delle competenze necessarie alla gestione delle Smart Class.

Tra le buone pratiche, nel corrente a.s., si evidenzia l'attività proposta dai referenti STEM, proff. Mario Pittalis e Marcella Orrù, sull' utilizzo delle APP nella didattica: periodicamente i due docenti propongono ai colleghi nuove modalità e diversi programmi innovativi dopo averli sperimentati.

Il corpo docente partecipa di buon grado a corsi di formazione anche nell'ambito di piani nazionali e possiede generalmente una buona base di competenze e, nel caso delle figure di sistema, anche di carattere specialistico. È inoltre disponibile ad aggiornarsi per mantenere al passo la propria formazione, in rapporto al rinnovo della dotazione multimediali. E' convinzione condivisa che il percorso della formazione specifica sull'utilizzo delle TIC nella didattica deve diventare un processo permanente e che deve prevedere anche momenti di autoaggiornamento.

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, la nostra Scuola si avvale dell'Animatore Digitale, una figura di sistema, che con il TEAM digitale, la Dirigente scolastica e la D.S.G.A. opera per concretizzare gli obiettivi e le innovazioni del PSND nella vita scolastica.

L'Istituto "A.Gramsci", per quanto riguarda la formazione specifica dei docenti sull'utilizzo consapevole e sicuro di Internet, ha formato alcuni docenti referenti sul tema " Azioni di contrasto al bullismo e al cyberbullismo", attraverso corsi specifici diversi (Piattaforma Elisa, Hashtag Project etc.) e continui momenti di autoformazione.

La nostra scuola fa parte del progetto GENERIAMO PARITÀ che vede più scuole in rete impegnate in attività di contrasto a tutte le discriminazioni e ai pregiudizi di genere.

L'Animatore Digitale ed i docenti del Team promuovono l'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali, fornendo assistenza continua ai docenti dell'Istituto e indicazioni sull'autoformazione, organizzando o supportando l'organizzazione di eventi formativi ed informativi ed affiancando le commissioni ed i gruppi di lavoro in ogni singola attività realizzata dalla scuola per la parte relativa all'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.

Dopo aver valutato il fabbisogno formativo degli insegnanti sull'uso sicuro della Rete, il nostro Istituto ha aderito al progetto "Generazioni Connesse" (SIC ITALY), coordinato dal MIUR, formando alcuni docenti sui temi del progetto. In un'ottica di vera e propria programmazione, prevediamo nei prossimi anni di proseguire con azioni specifiche:

- sul sito dell'Istituto sarà predisposta un'area specifica per gli insegnanti con materiali formativi per l'aggiornamento sull'utilizzo consapevole e sicuro di Internet con i link e i materiali informativi del progetto "Generazioni connesse dove trovare ulteriori approfondimenti, spunti, aggiornamenti e strumenti didattici utili da usare con gli studenti e le studentesse, per ciascun ordine e grado di scuola
- monitoraggio delle azioni svolte per mezzo di momenti di valutazione.
- incontri con professionisti della scuola o con esperti esterni, enti/associazioni, etc.

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

Nella prevenzione dei rischi connessi ad un uso non consapevole delle TIC, così come nella promozione di un loro uso positivo e capace di coglierne le opportunità, è necessaria la collaborazione di tutti gli attori educanti, ognuno secondo i propri ruoli e le proprie responsabilità. Scuola e famiglia devono rinforzare l'alleanza educativa e promuovere percorsi educativi continuativi e condivisi per accompagnare insieme ragazzi/e e bambini/e verso un uso responsabile e arricchente delle tecnologie digitali, anche in una prospettiva lavorativa futura. L'Istituto garantisce la massima informazione alle famiglie di tutte le attività e iniziative intraprese sul tema delle tecnologie digitali, previste dall'ePolicy e dal suo piano di azioni, anche attraverso l'aggiornamento, oltre che del regolamento scolastico, anche del "Patto di corresponsabilità" e attraverso una sezione dedicata sul sito web dell'Istituto.

L'Istituto per sensibilizzare le famiglie sui temi della sicurezza online intende organizzare incontri aperti anche vagliando le offerte del territorio (come gli interventi promossi dalla Polizia Postale).

Questo approccio, già sperimentato con gli alunni di alcune classi, offre occasioni di confronto e discussione sui rischi rappresentati dall'uso di cellulari, smartphone social network e chat line o da un uso inappropriato di tali dispositivi senza un'adeguata formazione; le famiglie verranno chiamate a collaborare in modo particolare ed attento in un'ottica di prevenzione del cyberbullismo.

Sul sito scolastico, nella bacheca virtuale, saranno resi accessibili alle famiglie e ai ragazzi i materiali, tra cui guide in formato pdf e video dedicati al tema del Web sicuro e del bullismo e cyber bullismo.

Dal sito web dell'Istituto sarà inoltre possibile per le famiglie accedere, seguendo appositi link, ad altri siti o progetti che affrontano tali argomenti (ad esempio il progetto "Generazioni connesse" Fondazione Carolina, Educazione digitale. etc).

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.

Riferimenti puntuali saranno poi riportati, oltre che nel Regolamento d'Istituto, anche nel "Patto di corresponsabilità", con specifici rimandi alle tecnologie digitali e all'ePolicy. Riteniamo che aggiornare il "Patto di corresponsabilità" sia fondamentale

per informare e rendere partecipi le famiglie sul percorso che abbiamo iniziato ad intraprendere. In tale sezione verranno esplicitate: le regole sull'uso delle tecnologie digitali da parte dei genitori nelle comunicazioni con la scuola e con i docenti: mail, registro elettronico; le regole per gli studenti e le studentesse.

Questa maggiore collaborazione e condivisione degli interventi di formazione ci permetterà di avere maggiori chance di successo anche nel contrasto al bullismo e al cyberbullismo.

Il nostro piano d'azioni

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

- 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 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 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.

La scuola è chiamata ogni giorno a costruire le condizioni per un futuro migliore delle nuove generazioni. Questa sfida riguarda anche il "corretto trattamento dei dati personali", presupposto necessario per il rispetto della dignità delle persone, della loro identità e del loro diritto alla riservatezza.

Nelle scuole di ogni ordine e grado vengono trattate giornalmente numerose informazioni sugli studenti e le studentesse, sulle loro famiglie, sui loro problemi sanitari o di disagio sociale, o ad esempio sulle abitudini alimentari. A volte può bastare una lettera contenente dati sensibili (quelli più delicati) di un minore, o un avviso scolastico con riferimenti indiretti sulle condizioni di salute degli/le studenti/esse, per violare anche involontariamente la riservatezza e la dignità di una persona.

Per questo è importante che le istituzioni scolastiche, durante lo svolgimento dei loro compiti, rispettino la privacy, tutelando i dati personali che si trovano a trattare, in particolare quando sono coinvolti soggetti minorenni.

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

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

I dati personali sono tutte le informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, etc.

Fra questi, particolarmente importanti sono:

- i dati che permettono l'identificazione diretta di una persona, come i dati anagrafici
- i dati che permettono l'identificazione indiretta, come un numero di identificazione (ad es. il codice fiscale, l'indirizzo IP, il numero di targa);
- i dati rientranti in particolari categorie: si tratta dei dati cosiddetti sensibili, cioè quelli che rivelano l'origine razziale o etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, dati relativi alla salute o alla vita sessuale di una persona. Il Regolamento (UE) 2016/679 (articolo 9) ha incluso nella nozione anche i dati genetici, i dati biometrici e quelli relativi all'orientamento sessuale;
- i dati relativi a condanne penali e reati: si tratta dei dati cosiddetti giudiziari, cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad es. i provvedimenti penali di condanna definitiva, la liberazione condizionale, il divieto o obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato. Il Regolamento (UE) 2016/679 (articolo 10) ricomprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

Con l'evoluzione delle tecnologie digitali, altri dati personali hanno assunto un ruolo significativo, come quelli relativi alle comunicazioni elettroniche (via Internet o telefono) e quelli che consentono la geo-localizzazione, fornendo informazioni sui luoghi frequentati e sugli spostamenti di una persona.

Quando parliamo di protezione di dati personali è bene aver chiaro quali sono i ruoli e i termini che interessano le persone coinvolte, cominciando dall'interessato che è la persona fisica alla quale si riferiscono i dati personali (art. 4, paragrafo 1, punto 1), del Regolamento UE 2016/679); il titolare invece è la persona fisica, l'autorità pubblica, l'impresa, l'ente pubblico, privato o l'associazione che adotta le decisioni sugli scopi e sulle modalità del trattamento (art. 4, paragrafo 1, punto 7), del Regolamento UE 2016/679); mentre il responsabile, individuato specificatamente dal titolare, è la persona fisica o giuridica alla quale il titolare richiede di eseguire per suo conto specifici e definiti compiti di gestione e controllo del trattamento dei dati (art. 4, paragrafo 1, punto 8), del Regolamento UE 2016/679).

Il Regolamento medesimo ha introdotto la possibilità che un responsabile possa, a sua volta e secondo determinate condizioni, designare un altro soggetto c.d. sub-responsabile (art. 28, paragrafo 2).

Si intende per trattamento quindi qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati, applicate a dati personali o insiemi di dati personali.

Ad esempio: la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (art. 4, par. 1, punto 2, del Regolamento (UE) 2016/679).

Tutti i soggetti che procedono al trattamento dei dati personali altrui devono adottare particolari misure per garantire il corretto e sicuro utilizzo dei dati, questo vale anche per le Istituzioni scolastiche pubbliche che possono trattare solamente i dati personali necessari al perseguimento di specifiche finalità istituzionali, oppure quelli espressamente previsti dalla normativa di settore. Per tali trattamenti non sono tenute a chiedere il consenso degli/le studenti/esse.

Le scuole, sia pubbliche che private, hanno perciò l'obbligo di informare (tramite apposita informativa) gli interessati delle caratteristiche e modalità del trattamento dei loro dati, indicando i responsabili del trattamento. Gli interessati non sono solo gli/le studenti/esse, ma anche le famiglie e gli stessi insegnanti. Sul sito della nostra scuola, nella sezione PRIVACY, è pubblicata non solo l'informativa generica per gli utenti del sito, ma anche quelle specifiche per alunni e famiglie, per la didattica a distanza e quelle relative a ingresso secondo il protocollo COVID.

<https://www.icantoniogramscioggi.edu.it/index.php/privacy-e-sicurezza/privacy/liberatorie>

Vengono inoltre verificati almeno una volta all'anno i trattamenti, controllando se i dati trattati non siano eccedenti rispetto alle finalità perseguite. Il nostro istituto ha avviato già da anni il processo di pieno adeguamento al Regolamento UE 2016/679. Fra le azioni necessarie, alcune saranno poste in essere a breve, come il registro dei trattamenti dei dati, sia per il titolare che per il responsabile dei trattamenti, altre vengono già effettuate come la valutazione dei rischi sulla privacy: (definita nel regolamento Data Protection Impact Assessment o PIA) relativamente ad alcune tipologie di trattamento dei dati sensibili. Viene anche verificato sistematicamente che la richiesta di consenso sia chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato (art. 7.2), per esempio, all'interno di modulistica o sul sito web istituzionale prestando attenzione alla formula utilizzata.

La scuola non è tenuta a chiedere il consenso per il trattamento dei dati personali, ma il personale viene ufficialmente nominato Responsabile del trattamento dei dati, nella misura che compete alle varie figure professionali: docenti, amministrativi o ausiliari. Viene posta anche attenzione all'adeguamento delle idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti:

Per quanto riguarda il sito web istituzionale di riferimento, la migrazione dal suffisso

gov.it a edu.it è già avvenuta. Il sito è stato professionalmente progettato secondo i concetti di [privacy by default e by design](#); ed è protetto dal protocollo HTTPS (l'Hypertext Transfer Protocol Secure è un protocollo per la comunicazione su Internet che protegge l'integrità e la riservatezza dei dati scambiati online); un'altra misura di protezione è l'utilizzo di un sistema di cifratura quando il trattamento di dati lo richiede e un sistema di backup di salvataggio;

L'istituto è di notevole complessità, con 15 plessi distribuiti su 6 comuni le cui amministrazioni sono proprietarie degli immobili e titolari dei contratti di fornitura delle linee internet, ovviamente tutti diversi.

La messa a disposizione di una rete, cablata o wifi, per la didattica non è di semplice gestione e costituisce un costante work in progress suscettibile di miglioramenti a cui ci dedichiamo con attenzione. In molti dei plessi sono in funzione proxy e firewall per la protezione del flusso dei dati, ed è costante l'impegno a realizzare la piena messa in sicurezza di tutte le reti scolastiche anche con l'utilizzo di sistemi di filtraggio dei contenuti. Ci proponiamo anche di effettuare ulteriori corsi di formazione per il personale.

La questione della privacy e del trattamento dati è senza dubbio delicata e richiede attenzione e comunicazione esplicita fra titolare e interessati, specialmente in ambito scolastico dove si ha a che fare con dei minori e dove è necessario avere la sensibilità di operare con il distinguo che possono non sembrare immediati. Ad esempio la scuola non è tenuta a richiedere alle famiglie l'autorizzazione alle riprese fotografiche e video (ad es. in caso di gite scolastiche o recite), ma solo se esse sono realizzate a fini personali e non a fini di pubblicazione o divulgazione. L'autorizzazione è invece indispensabile quando si pubblica sul sito della scuola o sulle pagine dei social network.

In generale il Garante per la protezione dei dati personali stabilisce che "le scuole devono rendere noto alle famiglie e ai ragazzi, attraverso un'adeguata informativa, quali dati raccolgono e come li utilizzano.

Famiglie e studenti hanno il diritto di conoscere quali informazioni sono trattate dall'Istituto scolastico, farle rettificare se inesatte, incomplete o non aggiornate.

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.

In tal senso, il nostro Istituto si è adoperato per aggiornare via via la dotazione tecnologica a disposizione dei vari plessi, attraverso progetti e finanziamenti che hanno consentito la creazione di laboratori, smart classes nonché svariate iniziative didattiche e formative mirate all'alfabetizzazione informatica e, più in generale, alla formazione digitale degli utenti e del personale scolastico

Nello specifico, gli interventi tuttora in divenire prevedono:

- la sostituzione o aggiornamento dei sistemi interattivi presenti in tutte le aule, dall'infanzia alla secondaria;
- l'acquisto di tablet e PC da mettere a disposizione di studenti e personale scolastico per far fronte ad ogni necessità didattica e fornire gli strumenti anche a chi non può permettersene l'acquisto

- l'adeguamento della connettività e delle reti intranet presenti nei plessi. A tale proposito, la scuola è impegnata in un dialogo serrato con le varie amministrazioni comunali al fine di ottenere il migliore accesso possibile alla rete internet, mentre all'interno dei plessi si provvede a monitorare costantemente la situazione degli apparati e delle infrastrutture di connessione per garantire continuità e affidabilità nella fruizione della rete ai fini didattici.
- L'avvio di diversi progetti di "coding" e robotica, realizzati anche attraverso l'acquisizione di materiali e strumenti didattici adatti alle varie fasce d'età degli utenti, a partire dalla scuola dell'infanzia.

Un ambiente sicuro anche online

In inglese esistono due termini per parlare di sicurezza: il primo termine è safety e riguarda la prevenzione dei rischi, a partire dalla consapevolezza, conoscenza e preparazione per un uso consapevole delle tecnologie digitali. L'altro termine è security che, in relazione ad Internet e ai media, si riferisce a tutte quelle risorse tecnologiche che rendono sicuro l'ambiente digitale, dall'antivirus al firewall, da un protocollo di trasmissione dei dati sicuro (https) all'aggiornamento di software e sistemi operativi.

La scuola deve dunque considerare l'ambiente online alla stregua dell'ambiente fisico e valutarne tutti gli aspetti legati alla sicurezza nel momento in cui permette a studenti, studentesse e docenti l'accesso alla rete tramite i dispositivi della scuola, tramite la rete scolastica o tramite i dispositivi personali nel caso del BYOD (Bring your own device).

Rispetto al concetto di security, il nostro Istituto ha allo studio soluzioni efficaci atte a garantire una fruizione sicura della rete. Il plesso centrale, sede anche degli uffici di presidenza e segreteria, è stato dotato di firewall e la rete didattica è stata separata dalla linea dedicata all'amministrazione. Si sta provvedendo alla continua manutenzione degli antivirus esistenti di default nelle varie macchine a disposizione degli studenti; inoltre è in fase di monitoraggio la situazione complessiva delle password, firewall e filtri di navigazione relativi a modem, router e access point presenti nei vari plessi, passo importante per prevenire l'accesso indesiderato a contenuti inopportuni da parte degli utenti. Altro passo fondamentale sarà istruire percorsi formativi/informativi allo scopo di favorire una sempre maggiore consapevolezza e presa di coscienza rispetto ad un uso corretto e responsabile di tutte le risorse inerenti la rete, ivi compresi i social network quali ad esempio Telegram, Whatsapp, Instagram ecc.

E' inoltre necessario considerare anche la sicurezza di tutti gli aspetti che riguardano la gestione degli account degli utenti (in modo differenziato tra studenti, insegnanti e personale amministrativo), il filtraggio dei contenuti (possibilmente in modo differenziato in base all'età) e gli aspetti legali in relazione prevalentemente alla

privacy.

Problemi tecnici

Per superare la diffidenza nei confronti delle tecnologie a scuola e il divario nell'accesso, è necessario andare oltre la possibile prima barriera che ne inibisce un uso efficace da parte di tanti docenti: i problemi tecnici e la scarsa familiarità con la strumentazione.

Per affrontare proattivamente la questione, la nostra scuola provvede a pianificare interventi periodici di manutenzione e si occupa di formare gli insegnanti per permettere loro di affrontare e risolvere in autonomia tutte quelle situazioni e casistiche di mal funzionamento dei dispositivi che si possono presentare nella quotidianità. La parola d'ordine per quanto riguarda le tecnologie è sempre: "formazione". Formazione non solo sull'uso delle tecnologie digitali nella didattica, ma anche sul funzionamento e sull'uso stesso della tecnologia in sé, anche allo scopo di aiutare a familiarizzare con i dispositivi, laddove si presentano incertezze e difficoltà. Questi obiettivi rappresentano un impegno continuativo per l'animatore digitale, in costante collaborazione col Team digitale e con il tecnico, che si occupa delle manutenzioni straordinarie.

Checklist per la cybersecurity

- Mantenere separate le reti didattica e segreteria: importante per garantire maggiore sicurezza alle informazioni, gestendo in modo autonomo e con regole differenti le due reti grazie al firewall.
- Aggiornare periodicamente software e Sistema operativo: garantire che il sistema sia aggiornato lo protegge dalle aggressioni esterne e dalle vulnerabilità che emergono nel tempo.
- Definire la programmazione di backup periodici: cioè la copia e messa in sicurezza dei dati del sistema scolastico per prevenire la perdita degli stessi (possibilmente anche una copia offline).
- Garantire formazione adeguata allo staff, incluso il corpo docenti: la formazione deve riguardare la gestione dei dispositivi, la conoscenza delle regole basilari sulla sicurezza.
- Testare regolarmente le possibili vulnerabilità.
- Preparare piani di azione in risposta ai problemi più seri: è importante non dover improvvisare nel momento in cui si verifica un problema serio, ma avere un protocollo di azione.

- Predisporre la disconnessione automatica dei dispositivi, dopo un certo tempo di inutilizzo: se non è previsto uno stand-by, il dispositivo resta accessibile nel caso in cui qualcuno dimentichi di spegnerlo, con il rischio potenziale di accesso da parte di persone non autorizzate.
- Impostare il browser per l'eliminazione dei cookies alla chiusura: in questo modo si evita che qualcuno possa avere accesso ad account altrui senza autorizzazione.
- Minimizzare i privilegi amministrativi: solo poche persone autorizzate dovrebbero avere privilegi amministrativi. Studenti e la maggior parte dei docenti possono accedere con account con permessi limitati.
- Sviluppare il regolamento sull'uso delle tecnologie a scuola (policy di uso accettabile): deve riguardare chiunque abbia accesso alla Rete, studenti/esse, docenti, amministrazione e segreteria, includere i dispositivi della scuola e quelli personali, anche in caso di BYOD.

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.

Un grande sforzo in questa direzione è stato fatto dalla nostra scuola, che in questi ultimi due anni ha approfittato dei finanziamenti stanziati dallo Stato per potenziare notevolmente la quantità di dispositivi tecnologicamente avanzati da mettere a disposizione di docenti e studenti, nelle aule ma anche a casa. Sono stati infatti acquistati monitor interattivi per quasi tutte le classi della secondaria e della primaria, che peraltro già erano dotate di LIM, ma anche tablet e pc da fornire in comodato ad alunni con bisogni educativi speciali e non, e dei docenti. Sono state implementate due Apple smart class, un nuovo laboratorio digitale e acquistati kit per la didattica digitale, robotica, coding e molto altro, programmando in maniera verticale per coinvolgere tutti i bambini e i ragazzi, dalla scuola dell'infanzia alla secondaria di primo grado. La sfida, allora, è quella di conoscere al meglio tali strumenti, sfruttarne

le potenzialità e come sempre prevenire eventuali rischi correlati ad un uso poco consapevole degli stessi.

Grazie all'uso delle tecnologie digitali, da una comunicazione uno a molti, si può passare ad una comunicazione che per definizione può essere di molti a molti, multimediale, bidirezionale e interattiva. Ciò naturalmente può rappresentare un'opportunità significativa anche in termini di un maggiore coinvolgimento degli studenti o dei genitori, o alla possibilità di usare diversi linguaggi (scrittura, immagini, video etc.) ma in taluni casi può anche rivelarsi un problema non sempre facile da gestire e per cui servono indicazioni chiare e condivise.

Le caratteristiche della comunicazione mediata dalle tecnologie

Quando ci relazioniamo attraverso l'uso di strumenti di comunicazione online, mettiamo in atto una modalità comunicativa che ha caratteristiche e logiche proprie. Per questo è essenziale che tutti gli appartenenti alla comunità scolastica siano consapevoli degli aspetti importanti di questo tipo di comunicazione che è importante tenere in considerazione. Come istituzione scolastica siamo partiti da una base immedita: ci siamo dotati di Regolamenti che specifichino in maniera chiara cosa si può fare e cosa no quando si comunica online. In un'apposita sezione del sito scolastico abbiamo inserito il Regolamento d'Istituto con le diverse declinazioni, dedicate per esempio alla DDI, agli organi collegiali a distanza ma anche al Cyberbullismo.

Come strumento di comunicazione esterna viene utilizzato quindi essenzialmente il sito web d'istituto dove in varie aree sono fornite le comunicazioni obbligatorie come in AMMINISTRAZIONE TRASPARENTE o ALBO PRETORIO, ma anche indicazioni sulla scuola, la sua organizzazione e gestione, i vari plessi che la compongono e le attività che si svolgono. Un'area importante è quella dedicata ai Documenti D'Istituto come il RAV, il PTOF e il PDM, mentre sono messe in evidenza circolari e iniziative speciali di interesse per le famiglie.

Fra gli strumenti di comunicazione interna, viene utilizzata la classica e-mail e, per praticità e diffusione, anche gli strumenti di messaggistica istantanea come whatsapp.

Questi però hanno sempre più funzionalità tipiche dei social network, per cui necessitano di una netiquette da condividere e diffondere: spesso non è chiara la differenza fra l'uso che se ne può fare per svago e, invece, per servizio. L'uso per servizio, implica che venga riconosciuto il "diritto alla disconnessione". L'art. 22 (Livelli, soggetti, materie di relazioni sindacali per la Sezione Scuola) del CCNL 2016/2018, infatti, fa riferimento ai criteri generali per l'utilizzo di strumentazioni tecnologiche di lavoro in orario diverso da quello di servizio, al fine di una maggiore conciliazione fra vita lavorativa e vita familiare. È importante sottolineare però che per le chat informali fra colleghi, o fra docenti e genitori, non esiste una vera e propria regolamentazione, e per tale ragione è fondamentale, a partire dal buon senso e da una riflessione sulle peculiarità del mezzo, che si elaborino regole condivise sull'uso

delle stesse mettendo in chiaro fin dall'inizio che è importantissimo:

- comprendere e rispettare sempre le finalità del gruppo, scrivendo e pubblicando solo contenuti pertinenti a tali finalità;
- Usare sempre un linguaggio adeguato e il più possibile chiaro e preciso
- Evitare di affrontare in chat argomenti troppo complessi e controversi;
- Evitare discussioni di questioni che coinvolgono due o pochi interlocutori, onde evitare di annoiare e disturbare gli altri componenti del gruppo;
- Non condividere file multimediali troppo pesanti;
- Evitare il più possibile di condividere foto di studenti in chat;
- Indirizzare solo domande precise e chiare, a cui si possano dare risposte altrettanto brevi e precise;
- Evitare messaggi troppo spezzettati, cercando il più possibile di essere brevi ed esaustivi allo stesso tempo.

La nostra scuola intende dotarsi di un vademecum, chiaro e possibilmente accattivante, per la diffusione delle regole da osservare quando si utilizza Whatsapp, prendendo ispirazione dalle iniziative analoghe prese con successo da altre scuole.

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

Altro strumento ormai centrale a disposizione delle scuole per la gestione di assenze, presenze, valutazioni, prenotazioni di incontri e comunicazioni con le famiglie è il registro elettronico.

La nostra scuola ha adottato il registro Argo. Con tutte le sue funzionalità e applicativi è lo strumento più idoneo per un'efficace e protetta comunicazione con le famiglie. Attraverso di esso le famiglie possono visualizzare molte informazioni utili, interagendo con la scuola, su:

- andamento scolastico (argomenti lezioni e compiti, note disciplinari);
- assenze (visualizzazione e giustificazione);
- risultati scolastici (voti, documenti di valutazione);
- udienze (prenotazioni colloqui individuali);
- eventi (agenda eventi);
- comunicazione varie (comunicazioni di classe, comunicazioni personali).

Il nostro istituto ha un referente dedicato per il registro elettronico e una mail specifica a cui i genitori possono chiedere assistenza. Vengono anche prodotti e diffusi tutorial che guidano docenti e genitori per alcune funzionalità chiave un po' più complesse, come la prenotazione colloqui o la nuova valutazione nella scuola primaria. Viene utilizzato in maniera estesa dalla stragrande maggioranza delle famiglie anche nella scuola dell'infanzia, cosa che non è comune.

Gli insegnanti lo utilizzano anche per la condivisione dei documenti, come le programmazioni o le unità didattiche e per la gestione delle proprie assenze. Anche i docenti a tempo determinato vengono accolti e guidati in maniera attenta all'utilizzo corretto e trasparente dello stesso.

Strumento non meno importante, dal 2020, vista la necessità di effettuare lezioni a distanza, la nostra scuola si è dotata di una propria versione virtuale e a questo scopo ha scelto di adottare una piattaforma prettamente didattica: Moodle, costruita su un dominio di proprietà dell'istituto, in modo che i dati forniti e scambiati fossero sempre e solo appartenenti all'istituto. Su Moodle sono presenti le versioni on line di tutte le classi e, in periodo di lezioni in presenza viene utilizzata in molti casi nella didattica integrata, per attività innovative.

Infine Google workspace integra le funzionalità a disposizione del personale docente per le comunicazioni interne, con le mail istituzionali e le funzionalità soprattutto per i meeting ristretti come i consigli di classe e che vengono organizzati on line in larga misura. Viene infine utilizzata la piattaforma GoToMeeting per i collegi docenti che contano oltre i 140 partecipanti. Per tutti questi strumenti, è fornita la debita informativa e sono stati attuati diversi momenti formativi per il corretto e sicuro utilizzo.

3.4 - Strumentazione personale

I dispositivi tecnologici sono parte integrante della vita personale di ciascuno, compresa quella degli/le 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.

Nel DPR 24 giugno 1998, n. 249 "Regolamento recante lo Statuto delle studentesse e degli studenti della scuola secondaria" (in GU 29 luglio 1998, n. 175), all'art. 2 (sezione Diritti), punto 8 lettera e si sottolinea "la disponibilità di un'adeguata strumentazione tecnologica" di cui la scuola deve dotarsi per offrirla ai propri studenti e alle studentesse che, d'altra parte, "sono tenuti ad avere nei confronti del capo d'istituto, dei docenti, del personale tutto della scuola e dei loro compagni lo stesso rispetto, anche formale, che chiedono per se stessi" (Art. 3, punto 2 sezione Doveri).

Più specificatamente, è nel DECRETO DEL PRESIDENTE DELLA REPUBBLICA 21 Novembre 2007, n. 235 "Regolamento recante modifiche ed integrazioni al decreto del Presidente della Repubblica 24 giugno 1998, n. 249", concernente lo statuto delle studentesse e degli studenti della scuola secondaria, che si introduce il Patto educativo di corresponsabilità e giornata della scuola (Art. 3) che definisce, attribuendole, le responsabilità fra istituzione scolastica e famiglia. Oggi, il Patto va letto anche in riferimento all'educazione dei ragazzi e delle ragazze all'uso dei nuovi dispositivi tecnologici, inclusi tablet e smartphone sia a scuola che a casa.

All'interno di tale cornice normativa, si inserisce la circolare n° 362 del 25 agosto 1998 "Uso del telefono cellulare nelle scuole" che ha come oggetto particolare l'uso del cellulare a scuola da parte dei docenti anche durante le ore di lezione. La circolare contiene tali orientamenti: "è chiaro che tali comportamenti - laddove si verificano - non possono essere consentiti in quanto si traducono in una mancanza di rispetto nei confronti degli alunni e recano un obiettivo elemento di disturbo al corretto svolgimento delle ore di lezione che, per legge, devono essere dedicate interamente all'attività di insegnamento e non possono essere utilizzate - sia pure parzialmente - per attività personali dei docenti". Un orientamento, dunque, volto a punire l'uso personale del dispositivo solo per il corpo docente.

La DM n. 30 del 15/03/2007 "Linee di indirizzo ed indicazioni in materia di utilizzo di telefoni cellulari e di altri dispositivi elettronici durante l'attività didattica, irrogazione di sanzioni disciplinari, doveri di vigilanza e di corresponsabilità dei genitori e dei docenti", invece, si concentra su più elementi che interessano, questa volta, anche gli studenti e le studentesse in un'ottica non punitiva ma risarcitoria e riparatoria.

In prima battuta, si ribadiscono alcuni doveri contenuti nell'articolo 3 del D.P.R. n. 249/1998: "per ciascuno studente, di non utilizzare il telefono cellulare, o altri dispositivi elettronici, durante lo svolgimento delle attività didattiche, considerato che il discente ha il dovere:

- di assolvere assiduamente agli impegni di studio anche durante gli orari di lezione (comma 1);
- di tenere comportamenti rispettosi degli altri (comma 2), nonché corretti e coerenti con i principi di cui all'art. 1 (comma 3);
- di osservare le disposizioni organizzative dettate dai regolamenti di istituto

(comma 4)" (DM n. 30 del 15/03/2007 - "Linee di indirizzo ed indicazioni in materia di utilizzo di telefoni cellulari e di altri dispositivi elettronici durante l'attività didattica, irrogazione di sanzioni disciplinari, doveri di vigilanza e di corresponsabilità dei genitori e dei docenti").

In seconda battuta, si sottolinea l'importanza del Patto educativo di corresponsabilità condividendo diritti e doveri fra scuola e famiglia la quale deve impegnarsi "a rispondere direttamente dell'operato dei propri figli nel caso in cui, ad esempio, gli stessi arrechino danni ad altre persone o alle strutture scolastiche o, più in generale, violino i doveri sanciti dal regolamento di istituto e subiscano, di conseguenza, l'applicazione di una sanzione anche di carattere pecuniario".

Resta la responsabilità deontologica e professionale dei dirigenti, dei docenti e del personale ATA che hanno il dovere di vigilare sui comportamenti degli studenti e delle studentesse il quale sussiste in tutti gli spazi scolastici e di segnalare eventuali infrazioni suscettibili di sanzioni disciplinari.

Nel nostro regolamento d'Istituto sono state opportunamente inserite sanzioni disciplinari in caso di uso scorretto dei cellulari da parte dei ragazzi e delle ragazze in classe, ma si programma e si lavora anche alla prevenzione in tutti gli ordini di scuola.

Con la DM n. 104 del 30/11/2007 "Linee di indirizzo e chiarimenti sulla normativa vigente sull'uso di telefoni cellulari e di altri dispositivi elettronici nelle comunità scolastiche" si chiarisce, anche in virtù della normativa allora vigente posta a tutela della privacy, il divieto di utilizzo di telefoni cellulari o di altri dispositivi elettronici nelle comunità scolastiche allo scopo di acquisire e/o divulgare immagini, filmati o registrazioni vocali. In altre parole, è punibile sia a livello civile che penale (oltre che le sanzioni previste dagli artt. 3 e 4, d.P.R. 24 giugno 1998, n. 249 - "Regolamento recante lo statuto delle studentesse e degli studenti della scuola secondaria"), chi abusa dei dati personali altrui raccolti (immagini, filmati, registrazioni vocali...), [violandone la privacy](#).

E proprio riguardo il Codice della Privacy, Digs. 196/2003, modificato e integrato dal D. Lgs. 101/2018 recependo il regolamento UE 2016/679 e art.10 del Codice Civile, è necessario considerare che "l'uso di cellulari e smartphone è in genere consentito per fini strettamente personali, ad esempio per registrare le lezioni, e sempre nel rispetto delle persone. Spetta comunque agli istituti scolastici decidere nella loro autonomia come regolamentare o se vietare del tutto l'uso dei cellulari. Non si possono diffondere immagini, video o foto sul web se non con il consenso delle persone riprese. È bene ricordare che la diffusione di filmati e foto che ledono la riservatezza e la dignità delle persone può far incorrere lo studente in sanzioni disciplinari e pecuniarie o perfino in veri e propri reati. Stesse cautele vanno previste per l'uso dei tablet, se usati a fini di registrazione e non soltanto per fini didattici o per consultare in classe libri elettronici e testi on line".

La riproduzione dei dati deve, pertanto, rispondere alla sola esigenza di

documentazione dell'attività didattica previa informativa e autorizzazione firmata o esplicito consenso (sono comprese le recite, i saggi scolastici e le gite raccolte dai genitori che non si configurano come violazione della privacy se raccolti per fini personali, familiari e non vengono pubblicate on line, in particolare sui social network).

A tal proposito, è bene ricordare la Legge n. 71 del 2017 "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo" che ancor di più cerca di contrastare manifestazioni comportamentali di soggetti minorenni a danno di altri minorenni che pongono "in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo" attraverso le tecnologie digitali. Dove anche gli adulti tutti, docenti e genitori, hanno responsabilità specifiche oltre che un ruolo di vigilanza e di educazione dei minori stessi.

Le disposizioni che si sono adottate in passato hanno perciò chiuso ad ogni possibilità di utilizzo misto dei dispositivi personali nelle attività didattiche come strumenti di socialità positiva e di occasione per l'educazione alle tecnologie digitali.

La questione qui descritta è stata affrontata, per la prima volta in maniera integrata, nel Piano Nazionale Scuola Digitale emanato dal Miur con la Legge 107 del 2015: "al fine di sviluppare e di migliorare le competenze digitali degli studenti e di rendere la tecnologia digitale uno strumento didattico di costruzione delle competenze in generale, il Ministero dell'istruzione, dell'università e della ricerca adotta il Piano nazionale per la scuola digitale (...)".

L'attenzione verso le tecnologie digitali e il loro utilizzo in classe diventa così inclusivo e creativo, nel senso che le stesse vengono riproposte come strumenti da inserire nella didattica e nelle sperimentazioni laboratoriali. L'uso viene consentito per scopi prettamente didattici, sotto il controllo e la responsabilità del docente che pianifica l'attività didattica.

["La scuola digitale, in collaborazione con le famiglie e gli enti locali, deve aprirsi al cosiddetto BYOD \(Bring Your Own Device\), ossia a politiche per cui l'utilizzo di dispositivi elettronici personali durante le attività didattiche sia possibile ed efficace"](#).

BYOD letteralmente significa "porta il tuo dispositivo" ed è un'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, gli smartphone, i tablet e i pc personali possono essere integrati nel lavoro nelle classi quando ben progettato e calibrato per discipline e obiettivi formativi e didattici: si pensi, a titolo di esempio, agli student response systems ossia alla possibilità degli studenti e delle studentesse di rispondere a quiz e sondaggi utilizzando direttamente il proprio smartphone come telecomando sempre sotto la guida e il controllo dell'insegnante.

A tale scopo, il MIUR, in collaborazione con AGID (l'Agenzia per il Digitale) e il Garante per la Privacy, ha elaborato apposite linee guida per promuovere il 3.4.

Strumentazione personale Si tratta di un vero e proprio decalogo che apre alla didattica integrata tramite un uso dei propri dispositivi personali in classe e alla sicurezza delle interazioni e delle relazioni fra pari tramite le tecnologie digitali.

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

1. Ogni novità comporta cambiamenti. Ogni cambiamento deve servire per migliorare l'apprendimento e il benessere delle studentesse e degli studenti e più in generale dell'intera comunità scolastica
2. I cambiamenti non vanno rifiutati, ma compresi e utilizzati per il raggiungimento dei propri scopi. Bisogna insegnare a usare bene e integrare nella didattica quotidiana i dispositivi, anche attraverso una loro regolamentazione. Proibire l'uso dei dispositivi a scuola non è la soluzione. A questo proposito ogni scuola adotta una Politica di Uso Accettabile (PUA) delle tecnologie digitali.
3. La scuola promuove le condizioni strutturali per l'uso delle tecnologie digitali. Fornisce, per quanto possibile, i necessari servizi e l'indispensabile connettività, favorendo un uso responsabile dei dispositivi personali (BYOD). Le tecnologie digitali sono uno dei modi per sostenere il rinnovamento della scuola.
4. La scuola accoglie e promuove lo sviluppo del digitale nella didattica. La presenza delle tecnologie digitali costituisce una sfida e un'opportunità per la didattica e per la cultura scolastica. Dirigenti e insegnanti attivi in questi campi sono il motore dell'innovazione. Occorre coinvolgere l'intera comunità scolastica anche attraverso la formazione e lo sviluppo professionale.
5. I dispositivi devono essere un mezzo, non un fine. È la didattica che guida l'uso competente e responsabile dei dispositivi. Non basta sviluppare le abilità tecniche, ma occorre sostenere lo sviluppo di una capacità critica e creativa.
6. L'uso dei dispositivi promuove l'autonomia delle studentesse e degli studenti. È in atto una graduale transizione verso situazioni di apprendimento che valorizzano lo spirito d'iniziativa e la responsabilità di studentesse e gli studenti. Bisogna sostenere un approccio consapevole al digitale nonché la capacità d'uso critico delle fonti di informazione, anche in vista di un apprendimento lungo tutto l'arco della vita.
7. Il digitale nella didattica è una scelta: sta ai docenti introdurla e condurla in classe. L'uso dei dispositivi in aula, siano essi analogici o digitali, è promosso dai docenti, nei modi e nei tempi che ritengono più opportuni.
8. Il digitale trasforma gli ambienti di apprendimento. Le possibilità di apprendere sono ampliate, sia per la frequentazione di ambienti digitali e condivisi, sia per l'accesso alle informazioni, e grazie alla connessione continua con la classe. Occorre regolamentare le modalità e i tempi dell'uso e del non uso, anche per imparare a riconoscere e a mantenere separate le dimensioni del privato e del pubblico.
9. Rafforzare la comunità scolastica e l'alleanza educativa con le famiglie. È

necessario che l'alleanza educativa tra scuola e famiglia si estenda alle questioni relative all'uso dei dispositivi personali. Le tecnologie digitali devono essere funzionali a questa collaborazione. Lo scopo condiviso è promuovere la crescita di cittadini autonomi e responsabili.

10. Educare alla cittadinanza digitale è un dovere per la scuola. Formare i futuri cittadini della società della conoscenza significa educare alla partecipazione responsabile, all'uso critico delle tecnologie, alla consapevolezza e alla costruzione delle proprie competenze in un mondo sempre più connesso.

La nostra scuola ritiene di assolvere al proprio dovere andando verso la responsabilizzazione di tutti i soggetti in gioco nel processo educativo e didattico, dove l'utilizzo delle tecnologie e dei dispositivi anche personali va mediato e calibrato sviluppando un pensiero critico.

L'ePolicy, documento di indirizzo e programmazione interno al progetto e insieme ai regolamenti previsti, viene redatto per identificare tali aspetti in termini di utilizzo del proprio smartphone a scuola e in classe, richiamando anche l'azione #15 del PNSD (Scenari innovativi per lo sviluppo di competenze digitali applicate) nell'ottica di potenziare le competenze di cittadinanza digitale.

In tale ottica, saranno integrati ulteriormente i Regolamenti già esistenti per disciplinare l'utilizzo delle TIC all'interno della scuola (es. la dotazione di filtri), e previste misure per prevenire diverse tipologie di rischio (non solo quelle più frequenti come il cyberbullismo) e stabilire procedure specifiche per rilevare e gestire le diverse problematiche.

Il nostro piano d'azioni

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

Scegliere almeno 1 di queste azioni:

- Organizzare uno o più eventi o attività volti a consultare i docenti dell'Istituto per redigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola
- Organizzare incontri per la consultazione degli studenti/studentesse su indicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della

protezione dei dati personali

- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali

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

Scegliere almeno 1 di queste azioni:

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli studenti e delle studentesse
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte dei docenti
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare i genitori dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

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

4.1 - Sensibilizzazione e Prevenzione

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

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

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

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

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

Il nostro istituto è impegnato in attività formative conformi (evidence-based) sia per la sensibilizzazione sia per la prevenzione.

1. SENSIBILIZZAZIONE.

Riteniamo fondamentale, al fine di sensibilizzare la comunità scolastica, una corretta informazione e formazione di tutti i professionisti coinvolti. Per questo il nostro Istituto, che è scuola capofila per la formazione dell'ambito 01-Sassari-Alghero-Goceano, nel corso delle ultime due annualità, ha previsto diversi moduli formativi destinati ai docenti:

(PIATTAFORMA ELISA per i docenti referenti, PREVENZIONE DELLE VIOLENZE DI GENERE, PRIVACY A SCUOLA, TECNOLOGIE DIDATTICHE E AMBIENTI DI APPRENDIMENTO INNOVATIVI, GESTIONE E CREAZIONE SITI WEB E BLOG CON WORDPRESS, DAD GSUITE E MICROSOFT 365, DAD E VALUTAZIONE, DALLA DAD (didattica a distanza) alla DDI (didattica digitale integrata), SMART CLASS APPLE, FLIPPED LEARNING APPROACH, CITTADINANZA DIGITALE, EDUCATIONAL FACT-CHECKING E CULTURA DIGITALE), che son stati proficuamente seguiti dalla molti insegnanti, non solo della nostra scuola.

Ma l'attivazione di una politica antibullismo richiede innanzitutto il coinvolgimento degli alunni e delle alunne, in modo che l'intervento venga percepito come partecipativo. Nel triennio precedente abbiamo attivato iniziative specifiche per singole classi, con interventi di professionisti psicologi e pedagogisti che lavorassero non solo in classe ma anche a livello formativo con i docenti. Questi interventi mancano però della sistematicità necessaria. Anche per questo intendiamo, fin da ora, aderire a programmi e progetti evidence-based quali il SIC di Generazioni Connesse, (progetto coordinato dal MIUR in partenariato con la Polizia Postale e delle Comunicazioni, l'Autorità Garante per l'Infanzia e l'Adolescenza, l'Università di Roma e di Firenze, Telefono Azzurro, Save the Children Italia, ecc), No Trap! (Noncadiamointrappola!) o la Campagna Nazionale Itinerante Una Vita da Social (in cui gli esperti della Polizia Postale incontrano, in un truck che fa tappa nelle città italiane, gli alunni di tutti gli ordini scolastici, i genitori e gli insegnanti).

Nelle nostre classi, la sensibilizzazione è programmata da molto tempo, fin dalle sezioni dell'infanzia, seppure non in maniera sistemica. Diventa sistemica a partire dalle classi quarte primaria e fino alle terze classi della secondaria di primo grado.

Gli obiettivi sono quelli di educare alla consapevolezza e alla riflessione e agire conseguentemente nella vita scolastica e di tutti i giorni; le tematiche principali sono:

- Utilizzo della rete e suo uso/abuso -
- Consapevolezza dei pericoli della rete-
- Dipendenza dallo smartphone

Si agisce in un'ottica di riflessione trasversale a tutte le discipline sia sul piano formativo sia sul piano conoscitivo (per es. nelle ore di EDUCAZIONE CIVICA); ma,

poiché la scuola promuove l'uso integrativo delle TIC nella didattica, preoccupandosi di farlo in sicurezza, si ritiene fondamentale mettere in atto un vero e proprio PIANO DI AZIONE e ciò sarà possibile solo attraverso l'ePolicy condivisa, che preveda la partecipazione attiva e responsabile di tutta la comunità scolastica ed educante attraverso azioni volte allo sviluppo delle competenze digitali, sociali e civiche e all'uso consapevole delle tecnologie digitali.

B)PREVENZIONE.

Gli interventi di prevenzione verranno portati avanti attraverso diversi percorsi, ciò significa che oltre a promuovere le competenze previste dal curriculum digitale un accento particolare viene dato:

- alla conoscenza dell'importanza di tutelare la propria privacy e quella degli altri (dati sensibili, password, foto, video) e dell'implicazioni legali in caso di trasgressione;
- alla conoscenza delle regole da tenere a mente quando si naviga in rete, quando si pubblica e/o si condivide un contenuto;
- alla riflessione su come sia possibile, dietro uno schermo apparentemente protetti dall'anonimato, infrangere con facilità tali norme, essere vittime o artefici di azioni lesive e offensive della propria e altrui persona.

Per quanto riguarda la prevenzione l'I.C. "A. Gramsci" adotta il modello su tre livelli che ritiene un'utile guida per affrontare e prevenire ogni possibile situazione di disagio:

Prevenzione Universale.

Questo tipo di interventi è diretto a tutti gli studenti ritenuti potenzialmente a rischio e non solo a quelli identificati sulla base di rischio individuale. Si tratta di programmi ad ampio raggio che possono produrre cambiamenti con un programma dedicato: alle competenze emotive e alla cittadinanza digitale. Insegnare le abilità sociali, incoraggiare la messa in atto di comportamenti di natura prosociale, lo sviluppo dell'empatia così come il riconoscimento e l'espressione delle emozioni, dei sentimenti, il ruolo del gruppo, quale risorsa fondamentale per fermare il bullismo, può migliorare le relazioni di classe e della scuola.

E' il settore a cui la nostra scuola si dedica maggiormente; nel corso dell'a.s 20/21 per esempio, per quanto riguarda il benessere a scuola e le competenze emotive, nella prima parte dell'a.s. (trimestre) hanno prestato servizio presso il nostro Istituto due psicologhe del progetto "Tutti a Scuola" (promosso e finanziato dalla Regione Sardegna), che hanno tenuto laboratori in presenza e on line e sportelli d'ascolto.

Così, anche in questo a.s. intende continuare: ponendo attenzione non solo all'approccio curricolare ma anche al potenziamento delle abilità emotive e sociali, alla

promozione della cooperazione, all'educazione e supporto tra pari, alla consulenza e mediazione dei conflitti.

Nella consapevolezza che i programmi antibullismo sono efficaci tanto più si fondano su un approccio di tipo ambientale e sistemico producendo cambiamenti nel clima scolastico, nelle regole e nei valori e promuovendo la collaborazione tra scuola, famiglia e risorse del territorio e il coinvolgimento degli alunni.

Prevenzione Selettiva.

È un programma dedicato a un gruppo di studenti per i quali il rischio sia presente.

Il programma si applica in quei casi in cui la prevenzione universale non abbia dato gli esiti previsti, o questi non siano sufficienti. Questi interventi sono mirati e prevedono programmi formativi strutturati che hanno l'obiettivo di migliorare le competenze digitali e le strategie di problem solving.

La presenza del rischio sarà individuata tramite: precedenti indagini, segnalazioni fatte dalla scuola, conoscenza della presenza di fattori di rischio nel territorio.

Anche per questo tipo di prevenzione si è data una prima risposta; infatti a partire da Gennaio 2021, per 120 ore, è stato promosso il progetto "Competenze emozionali e contrasto al bullismo e cyber bullismo", con incontri di formazione/informazione e laboratori a cura dello psicologo, con le classi più problematiche dell'istituto. La restituzione avuta (relazione con tabulazione dei dati acquisiti per ogni classe coinvolta) ci indica la strada per cui proseguire.

Prevenzione Indicata

È un programma di intervento sul caso specifico, pensato e strutturato per adattarsi agli/le studenti/studentesse. Per questo tipo di intervento è necessario avvalersi di professionalità diverse perché spesso affronta problemi legati alla salute mentale del minore per cui è opportuno coinvolgere anche la famiglia dell'alunn*.

Ha come obiettivo: ridurre e modificare i comportamenti problematici e dare supporto alle vittime.

Il modello su tre livelli è una guida sicura per affrontare e prevenire ogni possibile situazione di disagio.

Le azioni di sensibilizzazione, prevenzione e contrasto dei pericoli on line si svilupperanno innanzitutto attraverso la formazione/educazione curricolare nella quale verranno coinvolte direttamente le famiglie che implementeranno ulteriormente, nel rispetto del patto di corresponsabilità, lo sviluppo di una piena consapevolezza nelle diverse tematiche.

La responsabilità dell'azione preventiva ed educativa prevede anche la collaborazione di diverse agenzie educative, delle istituzioni, di diverse associazioni e della società civile. Tali agenzie verranno chiamate a collaborare ad un progetto comune, sia nell'ambito di funzioni educative condivise, in un'ottica di tutela dai rischi potenziali, che nella valorizzazione delle opportunità esistenti.

Sarà nostra cura strutturare soluzioni ed interventi mirati per rispondere a tutti i bisogni con strumenti e misure specifiche ed integrate, con procedure chiare (prevedendo accordi specifici) in collaborazione con la rete dei servizi locali (per esempio ASL e/o Polizia Postale).

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 nostro Istituto già nell'a.s 2019/20 si è dotato di un Regolamento per la Prevenzione e il Contrasto del Bullismo E Cyberbullismo (delibera n. 5 del Consiglio d'Istituto del 09/10/2019) di cui si può avere visione al link seguente: <https://urly.it/3gd7w> . Partendo dal presupposto che " Tutti gli alunni hanno diritto ad un sicuro ambiente di apprendimento e tutti devono imparare ad accettare e rispettare differenze di cultura e di personalità"(art.1) ritiene deprecabile e inaccettabile "Qualsiasi atto di cyber bullismo".

All'articolo 6 la seguente definizione:

"Sono da considerarsi comportamenti persecutori, contro il singolo o il gruppo, qualificabili come atti di CYBERBULLISMO:

- Flaming: litigi on line nei quali si fa uso di un linguaggio violento e volgare;
- Harassment: molestie attuate attraverso l'invio ripetuto di messaggi offensivi.
- Cyberstalking: invio ripetuto di messaggi che includono esplicite minacce fisiche, al punto che la vittima arriva a temere per la propria incolumità;
- Denigrazione: pubblicazione all' interno di comunità virtuali, quali newsgroup, blog, forum di discussione, messaggistica immediata, siti internet ecc., di pettegolezzi e commenti crudeli, calunniosi e denigratori;
- Outing estorto: registrazione delle confidenze, raccolte all' interno di un ambiente privato creando un clima di fiducia, poi inserite integralmente in un blog pubblico;
- Impersonificazione: insinuazione all'interno dell'account di un'altra persona, con l'obiettivo di inviare da tale account messaggi ingiuriosi che screditino la vittima;
- Esclusione: estromissione intenzionale dall'attività on-line;
- Sexting: invio di messaggi via smartphone e internet, corredati da immagini a sfondo sessuale".

All'art.4 vengono declinate le misure che guidano l'azione e l'organizzazione;se ne richiamano e si esplicitano, per brevità, le due ritenute essenziali:

1. creazione di un gruppo di lavoro sul bullismo-cyberbullismo coordinato dal

referente d'Istituto e dal team bullismo

2. iniziative di formazione e sensibilizzazione attraverso una progettualità che coinvolga tutta la comunità scolastica e realtà associative e istituzionali del territorio;

è stato costituito un gruppo di lavoro integrato, composto da 4 docenti adeguatamente formati, l'animatore digitale e dalla Dirigente scolastica; coordinato dalla Referente per la prevenzione bullismo/cyberbullismo, che ha i seguenti compiti:

Comunicazione interna: cura e diffusione di iniziative (bandi, attività concordate con esterni, coordinamento di gruppi di progettazione). Comunicazione esterna con famiglie e operatori esterni. Costituzione del documento di Epolicy di istituto. Raccolta e diffusione di documentazione e buone pratiche. Progettazione di attività specifiche di formazione. Attività di prevenzione per alunno. Sensibilizzazione dei genitori e loro coinvolgimento in attività formative. Partecipazione ad iniziative promosse dal MIUR, USR ed Enti locali.

Sarà costituito inoltre un Team per l'Emergenza, anche tramite reti di scopo, integrato da figure specializzate del territorio, sia perché non si dispone di uno psicologo scolastico fisso/interno (la presenza di questa figura di professionista, che dovrebbe essere sistemica nella scuola, in realtà dipende dai finanziamenti che vengono erogati annualmente), sia per favorire il coinvolgimento delle altre agenzie educative e di tutela dei minori, delle forze dell'ordine, dei servizi sanitari, delle strutture educative.

2- L'istituto "A. Gramsci" sensibilizza gli alunni attraverso la conoscenza organizzando eventi formativi/informativi con esperti esterni ed avviando percorsi educativi nelle classi anche nell'ambito dell'educazione civica.

La referente individuata nel nostro istituto, già da alcuni anni, ha acquisito le conoscenze utili a sviluppare le competenze richieste, a reperire strumenti e a produrre materiali da mettere a disposizione dell'intera comunità scolastica. Ritenendo di fondamentale importanza il coinvolgimento di tutte le componenti, nel corso di quest'anno scolastico avrà cura di predisporre una sezione del sito istituzionale della scuola con tutte le informazioni su siti, corsi di formazione e materiale vario, che, genitori, docenti, alunni e alunne potranno consultare, con una sottosezione che rimanda a: <https://www.generazioniconnesse.it/site/it/home-page/>, sito del MIUR, per informazioni di carattere generale.

Nel nostro Istituto il problema del cyberbullismo viene affrontato in classe dai docenti attraverso l'attivazione di percorsi di riflessione (PAROLE OSTILI;PENSO,PARLO,POSTO), sotto forma di colloqui di gruppo, visione di filmati

significativi (GENERAZIONI CONNESSE, FONDAZIONE CAROLINA, CUORI CONNESSI), giochi di ruolo etc., aspetti fondamentali per la prevenzione dei casi. Come già evidenziato, da diversi anni particolare cura si presta alla prevenzione di tipo universale e alla sensibilizzazione attraverso la sperimentazione di attività didattiche integrative e trasversali alle discipline per favorire lo sviluppo di competenze digitali, di legalità e cittadinanza attiva.

Tutti e tre gli ordini di scuola, a partire dall'infanzia, portano avanti specifiche unità di apprendimento e percorsi mirati sui temi del bullismo e cyber bullismo.

Grazie anche a progetti educativo-didattici specifici e/o di classe si affrontano tematiche importanti soprattutto per apportare reali cambiamenti in termini conoscenze e atteggiamenti degli alunni e delle alunne nei confronti dei fenomeni di bullismo e cyberbullismo.

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'Istituto "A. Gramsci" ha adottato il Manifesto della comunicazione Non Ostile, (<https://paroleostili.it>) promuovendo attività didattiche rivolte agli studenti e alle studentesse, supportate da un'adeguata formazione dei docenti e inserite nel curriculum

di educazione civica - cittadinanza digitale e nelle attività alternative all'IRC, volte a contrastare la diffusione di messaggi di incitamento all'odio sia su Internet che nel mondo offline .

Inoltre aderisce agli eventi commemorativi per la giornata contro la violenza sulle donne, la giornata della Memoria, la giornata del Ricordo, la giornata dell'Inclusione, la giornata dei Calzini spaiati, con proposizione alle classi di lavori in tal senso.

Come educatori ci proponiamo di far capire l'importanza delle parole utilizzate e le conseguenze che esse possono avere, anche nel mondo dei social network, dove spesso si leggono frasi che di persona non si avrebbe il coraggio di pronunciare. Nelle attività d'aula ci serviremo soprattutto di film, video (per esempio la mini-serie dei Super Errori, realizzata da Generazioni Connesse), articoli di giornale che affrontano questi argomenti.

Molto utile in classe potrebbe essere anche il manuale pratico "Silence Hate", per educare a contrastare il discorso d'odio, reperibile al seguente link <https://www.zaffiria.it/un-manuale-pratico-per-educare-a-contrastare-il-discorso-dodio-%EF%BB%BF/>

La nostra scuola prevede, inoltre, durante le ore curricolari, la condivisione di riflessioni individuali e di gruppo per 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, per promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network e per favorire una presa di parola consapevole e costruttiva.

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?

L'Istituto "A.Gramsci" promuove azioni di prevenzione con percorsi sul benessere digitale che integrano tecnologia e didattica, per rendere più consapevoli i ragazzi e le ragazze delle proprie abitudini online; aderisce volentieri ad iniziative ed eventi inerenti (proprio in queste settimane due classi hanno

partecipato ad una lezione online, proposta del Comune di Ossi, con attività varie che ha mostrato i limiti e gli inganni del gioco online); affronta quasi quotidianamente, nelle singole classi, la tematica del benessere digitale; ha regole specifiche e condivise attraverso il "Patto di Corresponsabilità" e il "Regolamento d'Istituto".

Utilizza, inoltre, alternative metodologiche e didattiche valide che costituiscono uno strumento fondamentale per non demonizzare la tecnologia o il gioco, stabilendo chiare e semplici norme di utilizzo.

Per quanto concerne la dipendenza da Internet ritiene fondamentale la collaborazione con le famiglie, in quanto gli studenti e le studentesse trascorrono il proprio tempo online soprattutto in orario extrascolastico; per cui progetteremo, possibilmente con la collaborazione degli EE.LL. una linea condivisa e informativa/formativa per i genitori, per evitare i pericoli che possono derivare da un uso eccessivo della Rete. (per esempio con le 3 A di Tisseron:Accompagnamento,alternanza e autoregolazione).

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 medialmente sessualmente espliciti; i/le ragazzi/e lo fanno senza essere realmente consapevoli di scambiare materiale (pedopornografico) che potrebbe arrivare in mani sbagliate e avere conseguenze impattanti emotivamente per i protagonisti delle immagini, delle foto e dei video.

Tra le caratteristiche del fenomeno vi sono principalmente:

la fiducia tradita: chi produce e invia contenuti sessualmente espliciti ripone fiducia nel destinatario, credendo, inoltre, alla motivazione della richiesta (es. prova d'amore richiesta all'interno di una relazione sentimentale);

la pervasività con cui si diffondono i contenuti: in pochi istanti e attraverso una condivisione che diventa virale, il contenuto a connotazione sessuale esplicita può essere diffuso a un numero esponenziale e infinito di persone e ad altrettante piattaforme differenti. Il contenuto, così, diventa facilmente modificabile, scaricabile e condivisibile e la sua trasmissione è incontrollabile;

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

La consapevolezza, o comunque la sola idea di diffusione di contenuti personali, si replica nel tempo e può finire con il danneggiare, sia in termini psicologici che sociali, sia il ragazzo/la ragazza soggetto della foto/del video che colui/coloro che hanno contribuito a diffonderla. Due agiti, quindi, che sono fra loro strettamente legati e che rappresentano veri e propri comportamenti criminali, i quali hanno ripercussioni negative sulla vittima in termini di autostima, di credibilità, di reputazione sociale off e on line. A ciò si associano altri comportamenti a rischio, di tipo sessuale ma anche riferibili ad abuso di sostanze o di alcool.

La Legge 19 luglio 2019 n. 69, all'articolo 10, ha introdotto in Italia il reato di "revenge porn", ossia la diffusione illecita di immagini o di video sessualmente espliciti.

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

L'Istituto negli anni scorsi ha affrontato la tematica sia trasversalmente nelle discipline sia nell'ambito del progetto di educazione alla salute, che organizzava, in special modo per gli/le alunni/e delle classi terze della Scuola Secondaria di Primo Grado, specifiche lezioni sull'educazione all'affettività e alla sessualità con figure professionali specializzate. In questi ultimi due anni le attività si sono interrotte. Ma, già da quest'anno si ristabilirà, anche con la collaborazione dell'ASL; ai docenti verranno segnalati eventuali corsi di formazione su questa tematica.

Per affrontare il tema del sexting con i/le ragazzi/e della secondaria di primo grado (classi II e III) nelle attività d'aula si utilizzano diversi film, discussioni su fatti di cronaca o video (per esempio "La Ragazza Visibile: l'inizio della storia" di Generazioni Connesse).

Per i prossimi anni verrà curata anche con la collaborazione di esperti esterni.

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.

L'Istituto porta avanti un percorso di educazione digitale che comprende lo sviluppo anche di capacità quali la protezione della propria privacy e la gestione dell'immagine e dell'identità online, la capacità di gestire adeguatamente le proprie relazioni online (a partire dalla consapevolezza della peculiarità del mezzo/schermo che permette a chiunque di potersi presentare molto diversamente da come realmente è) La problematica dell'adescamento online, come quella del sexting, si inquadra in uno scenario più ampio di scarsa educazione emotiva, sessuale e di assenza di competenza digitale, in riferimento al modo in cui i/le ragazzi/e vivono la propria sessualità e la propria immagine online, al loro desiderio di esprimersi e affermare se stessi.

La Scuola riguardo questa tematica richiede ai docenti, nelle attività d'aula di: fare prevenzione in classe attraverso il dialogo e la condivisione di film, video, articoli di giornale che trattano questa tematica; prestare attenzione anche a tutti i segnali (a volte anche piccoli) che possono essere rivelatori di problematiche più importanti (ad esempio cambiamenti improvvisi di umore, battute a sfondo sessuale nei confronti di un alunno/a...), partecipare ad eventuali corsi di formazione.

Per il nostro istituto è importante fornire, non solo agli alunni, ma anche ai genitori degli strumenti che consentano di monitorare le attività online del minore per un tempo consistente a partire dal momento in cui gli viene concessa la possibilità di navigare in modo solitario e di gestire autonomamente un proprio profilo sui social o di utilizzare una propria mail.

Se si sospetta o si ha la certezza di un caso di adescamento online è importante, innanzitutto, che l'adulto di riferimento non si sostituisca al minore nel rispondere, ad esempio, all'adescatore.

È importante che il computer o altri dispositivi elettronici del minore vittima non vengano usati per non compromettere eventuali prove. I casi di adescamento online richiedono l'intervento della Polizia Postale e delle Comunicazioni a cui bisogna rivolgersi il prima possibile, tenendo traccia degli scambi fra il minore e l'adescatore (ad esempio, salvando le conversazioni attraverso screenshot, memorizzando eventuali immagini o video...).

L'adescamento è, infatti, una problematica molto delicata da gestire e può avere ripercussioni psicologiche significative sul minore. Per questo potrebbe essere necessario rivolgersi ad un Servizio territoriale (es. Consultorio Familiare, Servizio di Neuropsichiatria Infantile, ecc.) in grado di fornire alla vittima anche un adeguato supporto di tipo psicologico o psichiatrico.

Per consigli e per un supporto è possibile rivolgersi alla Helpline di Generazioni Connesse (19.696): operatori esperti e preparati sono sempre a disposizione degli insegnanti, del Dirigente e degli operatori scolastici, oltre che dei bambini, degli adolescenti, dei genitori e di altri adulti che a vario titolo necessitano di un confronto e di un aiuto per gestire nel modo più opportuno eventuali esperienze negative e/o problematiche inerenti l'utilizzo dei nuovi media.

4.7 - Pedopornografia

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

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

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

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

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

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

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

Così come per il sexting e l'adescamento, il nostro Istituto ritiene che il miglior modo per prevenire tali fenomeni sia la formazione/informazione.

Pertanto si impegna ad accompagnare le ragazze e i ragazzi in un percorso di educazione all'affettività e alla sessualità per renderli più sicuri emotivamente e pronti ad affrontare eventuali situazioni a rischio, imparando innanzitutto a gestire le proprie emozioni, il rapporto con il proprio corpo e con gli altri. Si daranno a docenti, studenti e famiglie le indicazioni offerte dal progetto "Generazioni connesse" e i servizi da esso messi a disposizione.

Il nostro piano d'azioni

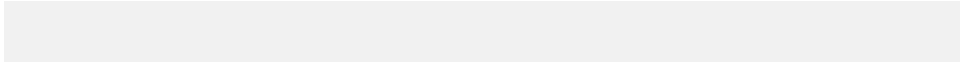
AZIONI (da sviluppare nell'arco dell'anno scolastico 2019/2020).

- Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse.
- 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/le studenti/studentesse.
- Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/le 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/le 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 laboratori di educazione alla sessualità e all'affettività, rivolti agli/le studenti/studentesse.
- Organizzare uno o più eventi e/o dibattiti in momenti extra-scolastici, sui temi della diversità e sull'inclusione rivolti a genitori, studenti/studentesse e personale della scuola.
- Pianificare e realizzare progetti di peer-education - sui temi della sicurezza online - nella scuola.



Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

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

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

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

Nelle procedure:

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

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

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

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

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

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

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

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

- **Cyberbullismo:** è necessario capire se si tratta effettivamente di cyberbullismo o di altra problematica. Oltre al contesto, vanno considerate le modalità attraverso le quali il comportamento si manifesta (alla presenza di un "pubblico"? Tra coetanei? In modo ripetuto e intenzionale? C'è un danno percepito alla vittima? etc.). È necessario poi valutare l'eventuale stato di disagio vissuto dagli/le 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 minorenni 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.

Gli alunni e le alunne, spesso, riferiscono o potrebbero riferire all'insegnante fatti o azioni personali o altrui, accaduti anche al di fuori della scuola, che il docente riconosce come pericolosi o potenzialmente pericolosi. La diffusione capillare dei social network tra i bambini e ancor più tra gli adolescenti, infatti, li espone sempre più spesso al rischio di inviare o condividere senza alcuna protezione materiali personali o riservati. Si considerano da segnalare tutte quelle situazioni che si configurano come:

episodi di cyberbullismo (caratterizzate da volontarie e ripetute aggressioni mirate a insultare, minacciare, diffamare e/o ferire una persona o un piccolo gruppo tramite un utilizzo irresponsabile dei social network); usi inappropriati della rete (siti d'odio, contenuti non adatti all'età degli alunni, ecc.); contenuti che violano della privacy (foto personali, l'indirizzo di casa o il telefono, informazioni private proprie o di amici, foto o video pubblicati contro la propria volontà, di eventi privati, ecc.); contenuti aggressivi o violenti (messaggi minacciosi, commenti offensivi, pettegolezzi, informazioni false, foto o video imbarazzanti, virus, contenuti razzisti, che inneggiano al suicidio, immagini o video umilianti, insulti, videogiochi pensati per un pubblico adulto, ecc.); contenuti afferenti alla sessualità: messaggi molesti, conversazioni (testo o voce) che connotano una relazione intima e/o sessualizzata, foto o video personali con nudità o abbigliamento succinto, immagini pornografiche, foto e video in cui persone di minore età sono coinvolte o assistono ad attività sessuali (pedopornografia), ecc.

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](tel:19696).

- Per aiutare insegnanti, studenti e studentesse e genitori a segnalare eventuali situazioni problematiche osservate all'interno della classe o nel plesso o nei propri figli, l'I.C. "Gramsci" prevede e mette loro a disposizione diversi strumenti di segnalazione:
- uno sportello in segreteria alunni per poter consegnare le schede di segnalazione;
- un indirizzo mail specifico;
- una scheda di segnalazione: <https://www.icantoniogramsciossi.edu.it/attachments/article/173/MODULO%20SEGNALAZIONE%20ATTI%20BULLSIMO-CYBERBULLISMO.pdf>
- un Protocollo: <https://www.icantoniogramsciossi.edu.it/attachments/article/173/PROTOCOLLO%20SEGNALAZIONE.pdf>
- una referente: prof.ssa Simonetta M. Schintu
- un'apposita Commissione di valutazione, con supervisione della DS: proff.: Maria Franca Campus, Salvatore Faedda, Gabriella Farina e Anna Marongiu.

- uno sportello di ascolto con psicologo d'Istituto (o in alcuni momenti dell'anno scolastico: quando, di solito i primi mesi, la Regione Sardegna finanzia "Tutti a Scuola" o su progetti di Istituto)

A CHI SEGNALARE Per quanto riguarda la gestione dei casi, il nostro Istituto ha individuato una figura referente per il bullismo/cyber bullismo che, coadiuvata dal gruppo di lavoro, si fa carico delle segnalazioni. In

realtà, la gestione dei casi rilevati andrà differenziata a seconda della loro gravità; in ogni caso è opportuna la condivisione a livello di Consiglio di Classe/Team di Docenti di ogni episodio rilevato. Alcuni avvenimenti di lieve entità possono essere affrontati e risolti con la discussione in classe. Altri casi ancora possono essere esaminati convocando genitori e alunno/a per riflettere insieme su quanto accaduto e individuare una strategia comune per affrontarlo e rimediare.

Per i casi più gravi bisogna informare la referente e segnalare, tramite modulo allegato al presente documento; il Team, si occuperà di raccogliere tutte le informazioni possibili, anche attraverso colloqui di approfondimento con gli attori coinvolti e di segnalare l'accaduto alla Dirigente. Sarà poi la Dirigente, insieme al Team, a valutare se la segnalazione debba essere rivolta ad organi esterni alla scuola quali la Polizia Postale o i Servizi Sociali o se il caso vada gestito all'interno della scuola con il coinvolgimento del Consiglio di Classe e delle famiglie degli alunni coinvolti.

Si sceglieranno uno o più interventi da attuare a cui seguirà una fase di monitoraggio.

Le azioni poste in essere dalla scuola saranno dirette non solo a supportare le vittime, le famiglie e tutti coloro che sono stati spettatori attivi o passivi di quanto avvenuto, ma anche a realizzare interventi educativi rispetto a quanti abbiano messo in atto comportamenti lesivi, ove si tratti di soggetti interni all'Istituto.

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.

Altri contatti utili per info, consulenza e segnalazioni in materia di bullismo e cyber bullismo. Online:

Garante Privacy:

<https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6732688>

La Polizia di Stato, per venire incontro alle diverse esigenze e consentire il disbrigo di determinate pratiche in maniera più agevole e veloce, ha realizzato il servizio di "Denuncia via web di reati telematici", un progetto che realizza un nuovo rapporto di collaborazione:

<https://www.commissariatodips.it/segnalazioni/index.html>.

POLIZIA POSTALE E DELLE COMUNICAZIONI SARDEGNA

Compartimento	Cagliari	Via Simeto, 38	- Tel. 070/27665
Sezione	Oristano	Via Canepa n.1	- Tel. 0783/210143
Sezione	Nuoro	Piazza Crispi, 1	- Tel. 0784/214266
Sezione	Sassari	Via Brigata Sassari, 13	- Tel. 079/2821239 /079 236631

INDIRIZZO PEC POLIZIA POSTALE SASSARI:
sez.polposta.ss@pecps.poliziadistato.it

INDIRIZZO MAIL POLIZIA POSTALE SASSARI: poltel.ss@poliziadistato.it (anche per segnalazioni anonime di casi specifici)

Il numero **114** è destinato a un servizio telefonico accessibile a chi vuole segnalare situazioni

emergenziali di disagio riguardanti l'infanzia e l'adolescenza. Il **114 Emergenza Infanzia** è attivo in tutta Italia, 365 giorni all'anno, 24 ore su 24. Il numero è gratuito sia da telefonia fissa sia da mobile.

Per i ragazzi sopra i 14 anni e gli adulti che vogliono esporre casi che coinvolgono dei minori, sono

attivi i numeri: 199.15.15.15 per chiamate da rete fissa e 02-55027304 per chiamate da cellulari e telefoni pubblici.

OSSERVATORIO NAZIONALE CYBERCRIME (Sardegna)

Consulenza psicologica, pedagogica, giuridica (gratuita) un servizio rivolto a studenti, docenti, genitori, operatori socio sanitari e giuridici nei casi di navigazione on line a rischio e cyberbullismo.

Tel. 070. 654382 Martedì e Venerdì dalle ore 15.00 alle ore 18.00 Via Sassari 3 - Cagliari

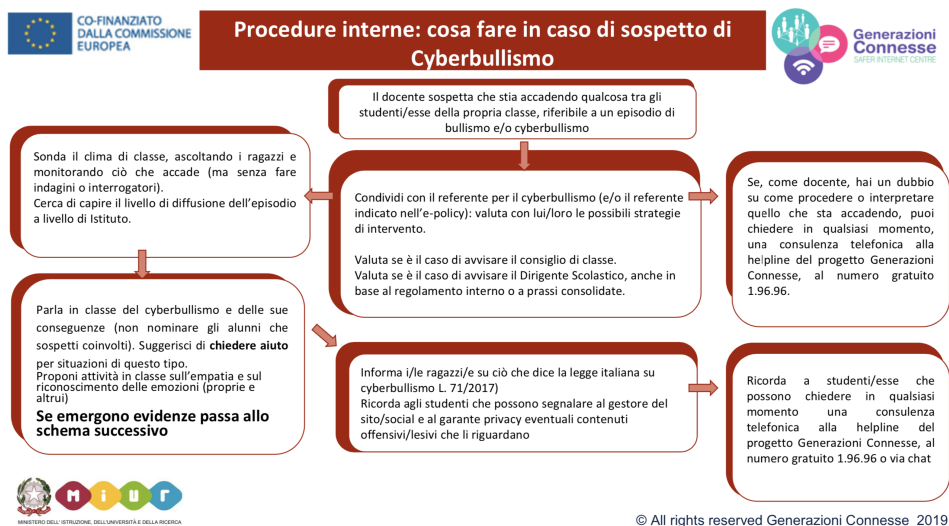
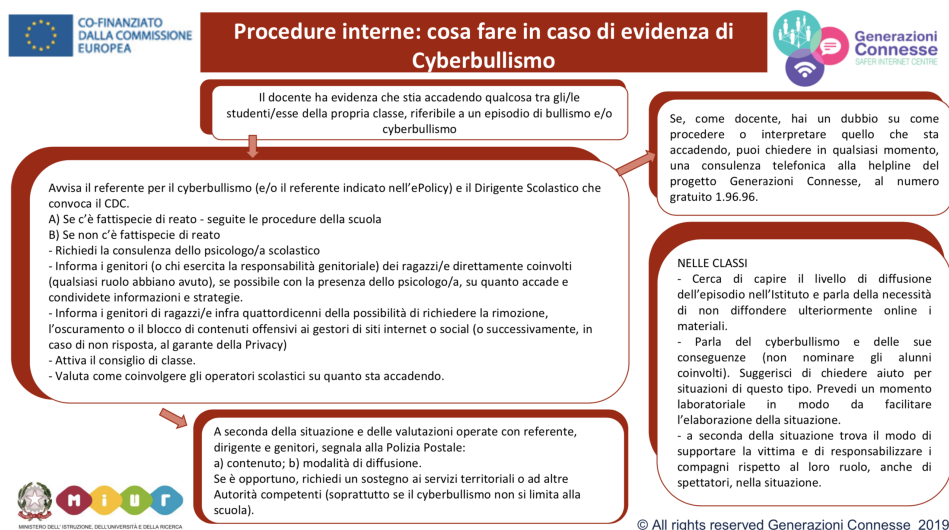
CONSULENZA DOCENTI: IFOS Tel. 070.883557 Email: info@cyberbullismo.com

CONSULENZA GENITORI/STUDENTI: IFOS Tel. 070.883557 Email: info@cyberbullismo.com.

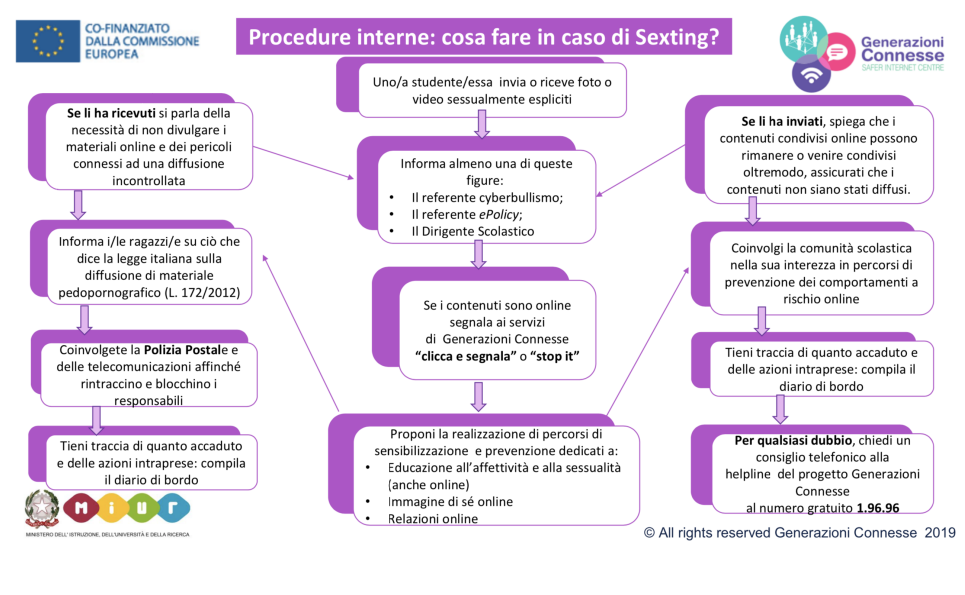
Per un'efficace gestione dei casi, i docenti si attengono alle modalità illustrate nello schema messo a disposizione da Generazioni Connesse (allegato).

5.4. - Allegati con le procedure

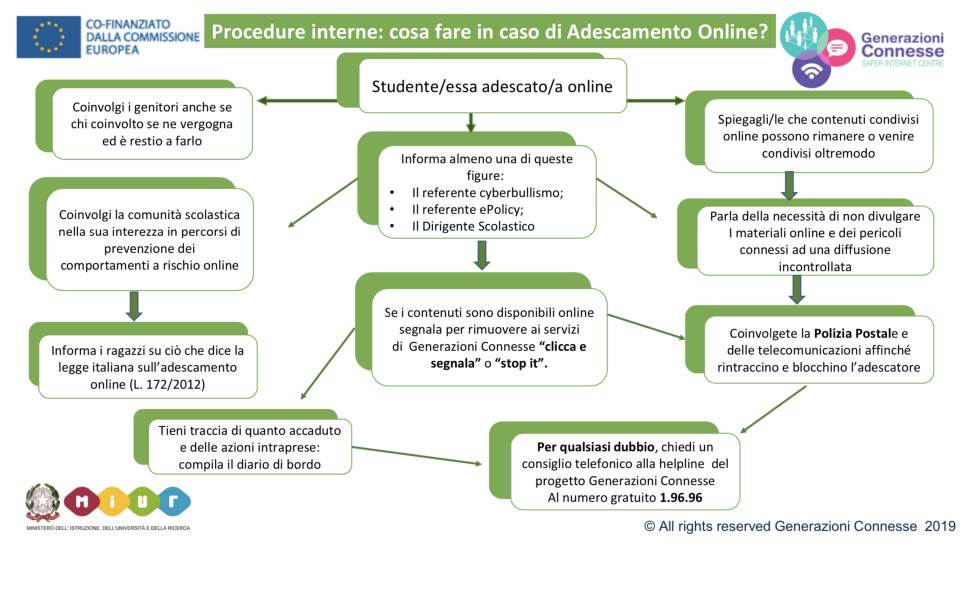
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



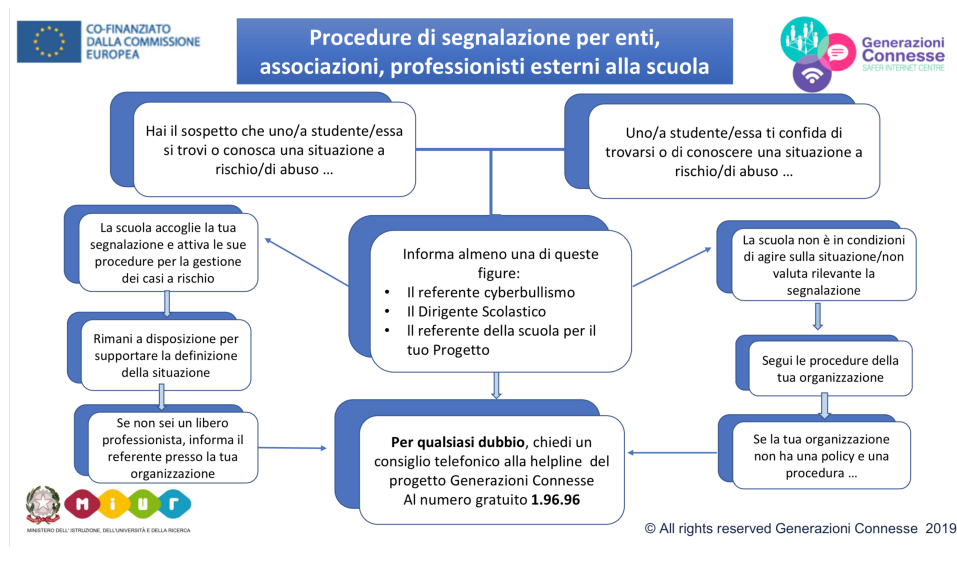
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



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



Altri allegati

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

Il documento programmatico dell'ePolicy, integrato nei vari regolamenti scolastici, sarà presentato,

promosso e disseminato,

con diversi mezzi di diffusione: l'utilizzo di locandine, nel sito della scuola;

in diversi momenti e ambiti scolastici ed extrascolastici: dipartimenti, collegi dei docenti, consigli di classe

riunioni formali e informali;

a tutti gli attori della comunità scolastica: genitori, studenti e studentesse, personale interno ed esterno.

Il nostro piano d'azioni

Adottare e diffondere le procedure e in generale questa e policy.

