Documento di ePolicy

TRIS009005

ORVIETO I.I.S. SCIENTIFICO E TECNICO

VIA DEI TIGLI - 05019 - ORVIETO - TERNI (TR)

Lorella Monichini

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

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.

Lo scopo fondamentale di questo documento consiste nel sensibilizzare tutta la comunità educante, intendendo con questo termine gli studenti, i docenti, le famiglie, il personale ATA e tutte le associazioni esterne o i professionisti che collaborano con la scuola, ad un utilizzo consapevole e corretto delle tecnologie, nel rispetto della dignità delle persone, dei regolamenti e della legge.

Il percorso di realizzazione del documento di ePolicy si inserisce a pieno titolo tra le iniziative di attuazione della Legge Legge 71/2017 "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo" e delle Linee guida per il contrasto al Bullismo e cyberbullismo del M.I.. Un utilizzo consapevole delle tecnologie significa, inoltre, garantire il rispetto della privacy e della sicurezza in rete, aspetto che sta particolarmente a cuore all'Istituto, impegnato su diversi fronti nell'educare tutta la comunità scolastica a riconoscere i rischi di un uso improprio e superficiale dei social network, soprattutto quando essi sostituiscono un dialogo aperto e costruttivo nella risoluzione di problematiche o disagi.

1.2 - Ruoli e responsabilità

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

Dirigente scolastico:

- Garantisce la tutela degli aspetti legali riguardanti la privacy e la tutela dell'immagine di tutti i membri dellacomunità scolastica;
- Garantisce ai propri docenti una formazione di base sulle tecnologie dell'Informazione e della Comunicazione (ICT) che consenta loro di possedere le competenze necessarie all'utilizzo di tali risorse;
- Garantisce l'esistenza di un sistema che consenta il monitoraggio e il controllo interno della sicurezza on- line;
- Informa tempestivamente, qualora venga a conoscenza di atti di cyberbullismo che non si configurino come reato, i genitori dei minori coinvolti; (o chi ne esercita la responsabilità genitoriale o i tutori)

- Regola il comportamento degli studenti ed impone sanzioni disciplinari in caso di comportamento inadeguato.

Referente Cyberbullismo d'Istituto:

- Coordina iniziative di prevenzione e contrasto del cyberbullismo messe in atto dalla scuola;
- Predispone un documento di rilevazione di incidenti di sicurezza in rete;
- Facilita la formazione e la consulenza di tutto il personale.

Animatore digitale e Team dell'innovazione:

- Pubblicano il presente documento di E-Policy sul sito della scuola;
- Diffondono i contenuti del documento tra docenti e studenti.

Insegnanti:

- Provvedono personalmente alla propria formazione/aggiornamento sull'utilizzo del digitale con particolare riferimento alla dimensione etica (tutela della privacy, rispetto dei diritti intellettuali dei materiali reperiti in internet e dell'immagine degli altri: lotta al cyberbullismo);
- Supportano gli alunni nell'utilizzo consapevole delle tecnologie informatiche utilizzate a scopi didattici;
- Segnalano al Dirigente Scolastico e ai suoi collaboratori eventuali episodi di violazione delle norme di comportamento stabilite dalla scuola, avviando le procedure previste in caso di violazione;
- Supportano ed indirizzano alunni coinvolti in problematiche legate alla rete.
- Può controllare ed accedere a tutti i file della intranet;
- È l'unico a poter istallare nuovi software;
- Limita attraverso un proxy l'accesso ad alcuni siti.

Direttore dei Servizi Generali e Amministrativi:

- Assicura, nei limiti delle risorse finanziarie disponibili, gli interventi di manutenzione necessari ad evitare un cattivo funzionamento della dotazione tecnologica dell'Istituto, controllando al contempo che le norme di sicurezza vengano rispettate.

Genitori:

- Contribuiscono, in sinergia con il personale scolastico, alla sensibilizzazione dei propri figli sul tema della sicurezza in rete;
- Incoraggiano l'impiego delle ICT da parte degli alunni nello svolgimento dei compiti a casa, controllando che tale impiego avvenga in sicurezza;

- Agiscono in modo concorde con la scuola per la prevenzione dei rischi e l'attuazione delle procedure previste in caso di violazione delle regole stabilite;
- Rispondono per gli episodi commessi dai figli minori a titolo di culpa in educando (articolo 2048 del Codice Civile). Sono esonerati da responsabilità solo se dimostrano di non aver potuto impedire il fatto.

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).

I soggetti esterni che sono responsabili di iniziative educative e formative nell'Istituto:

- prendono visione della politica dell'Istituto riguardo all'uso consapevole e responsabile della rete e delle TIC,
- promuovono la sicurezza on-line durante le attività di cui sono titolari,
- segnalano ai docenti preposti e al Dirigente Scolastico eventuali comportamenti problematici o casi di abuso nell'uso della rete e delle TIC.

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

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

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

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

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

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

In aggiunta a ciò, al fine di comunicare al meglio il documento di ePolicy a tutta la comunità scolastica, sono previste le seguenti azioni, da ripetersi con cadenza annuale:

- presentazione del documento ai docenti durante uno dei primi incontri del Collegio Docenti oppure durante uno specifico incontro di aggiornamento interno;

- presentazione del documento al personale A.T.A. durante uno specifico incontro di aggiornamento interno;

- presentazione del documento ai rappresentanti dei genitori e ai rappresentanti degli studenti durante specifici incontri, appositamente organizzati ad inizio anno scolastico;

- presentazione del documento a tutte le classi, ad inizio anno scolastico, inserendo l'argomento nella programmazione didattica, all'interno dell'educazione alla cittadinanza digitale, con test di valutazione finale sull'apprendimento e la comprensione 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.

In relazione all'uso improprio delle TIC a scuola da parte degli studenti e delle studentesse, sono sanzionate le seguenti condotte con gli strumenti disciplinari previsti dal regolamento e decisi dal Consiglio di Classe (sospensione, nota disciplinare, progetti, interventi di formazione, segnalazione alle autorità competenti etc):

- episodi di cyberbullismo;
- realizzazione e condivisione online, o anche solo condivisione, di immagini o video di compagni/e senza il loro consenso o che li ritraggono in pose offensive e denigratorie o comunque volti all'esclusione di compagni/e;
- realizzazione e condivisione, o anche solo condivisione, di scatti intimi e a sfondo sessuale;
- condivisione di dati personali di terzi (compagni, docenti, personale A.T.A.) senza il loro consenso;
- uso della rete per giudicare, infastidire o impedire a qualcuno di esprimersi o partecipare;
- condivisione in rete di comunicazione ufficiali interne all'Istituto: compiti in classe, circolari, comunicazioni, valutazioni e similari;
- registrazioni audio delle lezioni senza una preventiva autorizzazione da parte del docente;
- connessioni a siti proibiti o comunque non autorizzati;
- pirateria informatica;
- scaricamento di file (video, film, musica, immagini, test, ecc.) per finalità non didattiche.

In relazione all'uso improprio delle TIC a scuola in situazioni in cui gli studenti risultino "vittime", sono segnalate agli organi territoriali competenti le seguenti condotte:

- possibile dipendenza (patologica) dalla rete (social network, gambling, vamping,
- esposizione a filmati violenti o a contenuto pedopornografico;
- relazioni pericolose/adescamento in rete;
- incitazione all'odio;
- divulgazione di notizie false.

1.6 - Integrazione dell'ePolicy con Regolamenti esistenti

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

Il presente documento di ePolicy è allegato al Regolamento dell'Istituto scolastico e al Patto di Corresponsabilità, con opportuni riferimenti anche all'interno di tali documenti.

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 gruppo di lavoro costituitosi per la redazione del documento di ePolicy si occupa altresì della sua revisione e del suo aggiornamento periodico, ovvero almeno ogni due anni e qualora si verificassero cambiamenti significativi in riferimento all'uso delle tecnologie digitali all'interno della scuola.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

- Organizzare una riunione dei Coordinatori di Dipartimento per discutere delle attività relative all'ePolicy.
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto agli studenti;
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy

rivolto ai docenti;
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai genitori.

Azioni da svolgere nei prossimi 3 anni:

- Realizzazione di un sistema di monitoraggio delle attività di prevenzione e formazione (somministrazione a campione nelle classi prime sulle azioni di prevenzione del bullismo e del cyberbullismo);
- Monitoraggio dell'efficacia dell'ePolicy attraverso sondaggio rivolto a tutte le componenti dell'Istituto;
- Formazione del personale docente e non docente sui reati on-line e sulla privacy;
- Implementazione della dotazione tecnica delle classi, per quanto concerne LIM, PC, tablet (anche in comodato d'uso agli studenti) con particolare attenzione nei confronti degli allievi con BES, nei limiti delle dotazioni finanziarie dell'Istituto e dei fondi dedicati.
- Stesura di un curricolo digitale d'Istituto.
- 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

Capitolo 2 - Formazione e curricolo

2.1. Curricolo sulle competenze digitali per gli studenti

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

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

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

Il concetto di competenza rappresenta la capacità di utilizzare conoscenze, abilità e, in genere, tutto il proprio sapere, in situazioni reali di vita e lavoro. Le competenze digitali rientrano tra le otto competenze chiave che la Comunità Europea ha individuato per il pieno sviluppo della cittadinanza (Raccomandazioni del Parlamento Europeo e del Consiglio "Le competenze chiave per l'apprendimento permanente", 2006). La competenza digitale è una competenza trasversale, quindi tutti i docenti sono chiamati a promuoverla, come si evince dal profilo delle competenze in uscita dalla scuola secondaria superiore. L'obiettivo è quello di rispondere ai bisogni di conoscenza, di espressione e di comunicazione dei ragazzi e aiutarli a organizzare, riflettere, attribuire senso alla loro esperienza tecnologica, orientarsi per una nuova ecologia dei media verso la logica dell'integrazione, della non intrusività del mezzo, dell'uso non passivizzante della tecnologia, di una esperienza tecnologica consapevole.

In quest'ambito si seguono le indicazioni contenute nel PNSD (azione 14), in cui si

individuano alcuni *framework* di riferimento per la definizione e lo sviluppo delle competenze digitali, tra cui il *framework* DIGCOMP, che prevede 21 competenze, di cui alcune specifiche nell'area della sicurezza.

Partendo dal quadro di riferimento DIGCOMP verrà eleborato nel corso di questo anno scolastico un **curricolo digitale verticale** nel quale sono elencate le competenze da considerarsi come traguardi in uscita.

Aree di competenza:

- informazione
- comunicazione
- creazione di contenuti
- problem-solving
- sicurezza

Descrittori di competenza:

- Lo studente identifica, localizza, recupera, conserva le informazioni digitali secondo un approccio "intuitivo";
- Lo studente identifica, localizza, recupera le informazioni digitali con consapevolezza e con atteggiamento critico;
- conserva, organizza e analizza le informazioni digitali;
- Lo studente comunica in ambienti digitali, condivide risorse attraverso strumenti on-line, sa collegarsi con gli altri e collabora attraverso strumenti digitali, interagisce e partecipa alle comunità e alle reti;
- Lo studente realizza e modifica contenuti (da elaborazione testi a immagini e video), integra e rielabora conoscenze, produce contenuti in modo creativo;
- Lo studente utilizza gli strumenti digitali per identificare e risolvere piccoli problemi tecnici, contribuisce alla creazione di conoscenza, produce risultati creativi ed innovativi, supporta gli altri nell'uso degli strumenti digitali;
- Lo studente riflette e acquisisce consapevolezza su protezione personale, protezione dei dati, protezione dell'identità digitale, misure di sicurezza; conosce ed applica i diritti di proprietà intellettuale e le licenze.

Strumenti

- Rete e connettività
- Registro elettronico e ambiente di lavoro condiviso
- Google Workspace Education (Gmail, Google Drive, Classroom, …) come ambiente informatico ad accesso gratuito per la gestione e condivisione di materiale didattico, corsi, verifiche formative e sommative, prove comuni, consegne
- Video didattici in rete (es. YouTube, OVO, risorse digitali dei manuali in adozione, RAI Scuola, RAI Play)
- Software per la produzione di documenti, fogli di calcolo e presentazioni Software di geometria dinamica (es. Geogebra, Desmos, Tinkercad)

- Software per la didattica collaborativa (es. Padlet, Google Maps, EdModo, Weschool, Etwinning, Pik-to-chart, Storyboard that, Speak-Pic)
- Software per lo sviluppo del pensiero computazionale e il making educativo (es. Cura, pacchetto Autodesk)
- Software per la realizzazione di mappe concettuali (es. CMap) e video tutorial (Kdenlive)
- Software per videoconferenza (Meet)

Traguardi formativi

- Utilizzare la rete per scopi di informazione, comunicazione, ricerca e svago;
- Utilizzare strumenti informatici e di comunicazione per elaborare dati, testi e immagini e produrre documenti;
- Conoscere le caratteristiche e le potenzialità tecnologiche degli strumenti d'uso più comuni (PC, tablet, smartphone, strumenti archiviazione memoria digitale);
- Riconoscere vantaggi, potenzialità, limiti e rischi connessi all'uso delle tecnologie più comuni, anche informatiche Apprendere a utilizzare gli "aggregatori" digitali;
- Cogliere e sfruttare le potenzialità creative e non solo quelle funzionali delle applicazioni digitali Apprendere a discriminare le fonti di informazione più affidabili.

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.

Nel corso degli anni presso l'IISST Majorana-Maitani è stato favorito l'inserimento delle tecnologie informatiche nella didattica (registro elettronico, LIM, ambienti di condivisione) nella prospettiva dell'inclusione, non solo in relazione ai Bisogni Educativi Specifici, ma più in generale per facilitare un percorso di apprendimento in grado di promuovere il successo formativo offrendo risposte adeguate ed efficaci "a

tutti e a ciascuno". Tutto ciò nel rispetto della libertà di insegnamento e delle propensioni personali del singolo docente.

Si prevede l'attivazione di iniziative di formazione facendo ricorso a soggetti esterni e/o al personale docente interno alla scuola che abbia acquisito competenze sull'innovazione didattica. Il percorso della formazione specifica dei docenti sull'utilizzo delle TIC nella didattica deve diventare un processo permanente che deve prevedere anche momenti di autoaggiornamento, di formazione personale o collettiva.

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

La scuola si impegna a promuovere percorsi formativi per gli insegnanti sul tema dell'uso consapevole delle tecnologie digitali e della prevenzione dei rischi online. Ciò avverrà tramite specifici momenti di aggiornamento che, con cadenza, verranno organizzati dall'Istituto scolastico con la collaborazione del personale specializzato interno (animatore digitale, referente bullismo e cyberbullismo) e se necessario del personale esterno (professionisti qualificati), con il supporto della rete scolastica del territorio (USR, Osservatori regionali sul bullismo, scuole Polo, etc…), delle amministrazioni comunali, dei servizi socio-educativi e delle associazioni presenti.

Coerentemente con quanto previsto dal PNSD, l'Istituto si avvale dell'Animatore Digitale, che coordina la diffusione dell'innovazione digitale e collabora con tutti i soggetti che possono contribuire alla realizzazione degli obiettivi del Piano.

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.Parallelamente alla formazione sull'utilizzo del Tic, sarà organizzato almeno un corso di formazione interno annuale sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.

Negli anni passati l'Istituto con la collaborazione del personale della ASL Umbria ha formato alcuni membri del personale docente e circa 60 studenti sui temi del

cyberbullismo attraverso la metodologia della peer education.

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.

Con cadenza annuale sarà svolta un'analisi dei fabbisogni delle famiglie al fine di organizzare percorsi di sensibilizzazione e formazione dei genitori su un uso responsabile e costruttivo della Rete in famiglia e a scuola.

Il Patto di Corrsponsabilità è stato modificato ed integrato da una commissione apposita nell'anno scolastico 2021-20022.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2022/2023)

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

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

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

- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare incontri con esperti per i docenti sulle competenze digitali.
- Organizzare incontri con esperti per i genitori sull'educazione alla cittadinanza digitale.

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

3.1 - Protezione dei dati personali

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

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

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

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

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

In questo paragrafo dell'ePolicy affrontiamo tale problematica, con particolare

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

INFORMATIVA PER IL TRATTAMENTO DEI DATI PERSONALI ai sensi dell'art. 13 del Regolamento UE n. 2016/679

Identità e dati di contatto del titolare:
Il Titolare del trattamento Istituto Istruzione Superiore Scientifico e Tecnico con sede legale in via dei Tigli, snc Orvieto (TR), Tel. 0763/302198 Mail: tris009005@istruzione.it, PEC: tris009005@pec.istruzione.it, nella persona del suo legale rappresentante Prof.ssa LORELLA MONICHINI
2. Identità e dati di contatto di un eventuale rappresentante nominato dal titolare o dal responsabile del trattamento:
Il rappresentante del titolare è la Prof.ssa LORELLA MONICHINI i cui contatti sono: Tel. 0763/302198
Mail: tris009005@istruzione.it, PEC: tris009005@pec.istruzione.it.
3. Identità e dati di contatto del RDP/DPO (Responsabile della Protezione dei Dati/Data Protection Officer):
Il responsabile della protezione dei dati è Avv. MARTINI LUCA il cui contatto è:
Mail: avv.lucamartini@tiscali.it.
4. Oggetto del trattamento e natura dei dati:
Il Titolare tratta solo Dati personali identificativi strettamente necessari per perseguire la finalità di seguito descritta (Nome, cognome, data e luogo di nascita, codice fiscale dell'alunno, nome, cognome, data e luogo di nascita, codice fiscale, e-mail e numeri di telefono del genitore) da Lei comunicati in occasione della iscrizione.
5. Finalità del trattamento cui sono destinati i dati personali e base giuridica del trattamento:
I dati personali sono trattati:
Senza la necessità di un espresso consenso (Regolamento UE 2016/679 art. 6 lett. e) e f) "Liceità del trattamento"):
A) Tutti i dati personali forniti, in relazione al rapporto che intrattiene con la presente Istituzione scolastica, saranno trattati dal personale autorizzato esclusivamente per le finalità istituzionali della scuola che sono quelle relative all'istruzione ed alla formazione degli alunni e quelle amministrative ad esse strumentali.
- Banca dati ministeriale: SIDI;
- Conservazione in cloud presso il gestore di archiviazione della didattica – protocollo o altro software collegato: INFOSCHOOL SPAGGIARI, , COMUNE, PROVINCIA, - ENTE
B) Per essere sottoposto a valutazione di qualità da parte degli stakeholders dell'Istituto (personale interno, famiglie, sistema di qualità, istituzioni ministeriale, etc…);

C) Il Titolare potrà comunicare i Suoi dati per le finalità di cui all'art. 5 a Organismi di vigilanza, Autorità giudiziarie, società di assicurazione per la prestazione di servizi assicurativi, nonché a quei soggetti ai quali la comunicazione sia obbligatoria per legge per l'espletamento delle finalità dette. Questi soggetti tratteranno i dati nella loro qualità di autonomi titolari del trattamento;
D) I dati definiti come "dati personali" o come "dati particolari" dal Codice e i dati previsti dagli art. 9 e 10 del Regolamento saranno trattati esclusivamente dal personale autorizzato della scuola, appositamente incaricato, secondo quanto previsto dalle disposizioni di legge e di regolamento citate al precedente punto
a) e tassativamente nel rispetto del principio di stretta indispensabilità dei trattamenti;

E) La comunicazione dei dati richiesti è indispensabile e obbligatoria in quanto espressamente prevista dalla normativa citata al precedente punto; l'eventuale rifiuto a fornire tali dati potrebbe comportare il mancato perfezionamento, la gestione o l'interruzione del rapporto; i dati personali più sopra evidenziati potranno essere trattati, solo ed esclusivamente per le finalità istituzionali della scuola, anche se raccolti non presso l'Istituzione scolastica ma presso il Ministero dell'Istruzione e le sue articolazioni periferiche, presso altre Amministrazioni dello Stato, presso Regioni e enti locali, presso Enti con cui la scuola coopera in attività e progetti previsti dal Piano Triennale dell'Offerta Formativa;
F) Il trattamento potrà essere effettuato sia con strumenti cartacei che elettronici, nel rispetto delle misure di sicurezza individuate ai sensi del Regolamento; i dati verranno conservati nel rispetto delle Regole tecniche in materia di conservazione digitale degli atti definite da AGID e nei tempi e nei modi indicati dalle Linee Guida per le Istituzioni scolastiche e dai Piani di conservazione e scarto degli archivi scolastici definiti dalla Direzione Generale degli Archivi presso il Ministero dei Beni Culturali;
G) I "dati particolari", di cui all'art. 9, 1 Lettera a) Lettera b) del Regolamento, non saranno oggetto di diffusione; per svolgere attività istituzionali previste dalle vigenti disposizioni in materia sanitaria, previdenziale, giudiziaria e di istruzione, nei limiti previsti dal D.M 305/2006, pubblicato sulla G.U. n°11 del 15-01-07, alcuni di essi potranno essere comunicati ad altri soggetti pubblici solo se strettamente indispensabile;
H) I "dati comuni" potranno essere comunicati a soggetti pubblici (Ufficio scolastico regionale, Ambiti Territoriali, ASL, Comune, Provincia, organi di polizia giudiziaria, guardia di finanza, magistratura, ecc.) nei limiti di quanto previsto dalle vigenti disposizioni di legge e di regolamento e degli obblighi conseguenti per codesta istituzione scolastica;
I) I dati da Lei forniti potranno essere comunicati a soggetti terzi che forniscono servizi a codesta Istituzione Scolastica. L'effettuazione di questi trattamenti costituisce una condizione necessaria affinché l'interessato possa fruire dei relativi servizi; solo in caso di trattamenti effettuati in maniera continuativa e non saltuaria o occasionale, le aziende in questione saranno nominate Incaricati esterni del Trattamento, limitatamente ai servizi richiesti e resi;
J) Con riferimento ad attività didattiche afferenti gli scopi istituzionali della Scuola, inserite nel Piano dell'Offerta Formativa (quali ad esempio attività di laboratorio, visite

guidate, premiazioni, partecipazioni a gare sportive, ecc.) è possibile che delle foto vengano pubblicate sul sito istituzionale, canali social (quali ad esempio Facebook, Youtube, Istagram, Google, Twitter, Pinterest, ecc) e/o sul giornalino della scuola; è inoltre possibile che vengano effettuate durante l'anno foto di classe, riprese audio e video di lavori e manifestazioni, da parte della scuola, di alcune attività didattiche e istituzionali. In tal caso il trattamento avrà una durata temporanea in quanto tali materiali rimarranno esposti esclusivamente per il tempo necessario e per la finalità cui sono destinati. Nei video e nelle immagini di cui sopra i minori saranno ritratti solo nei momenti "positivi" (secondo la terminologia utilizzata dal Garante per la protezione dei dati personali e dalla Carta di Treviso del 5 ottobre 1990 e successive integrazioni) legati alla vita della scuola: apprendimento, recite scolastiche, competizioni sportive, ecc.

K) I dati da Lei forniti potranno essere comunicati a soggetti terzi che richiedano a codesta Istituzione Scolastica, informazioni per "Inserimento Professionale".

L) Si fa presente che per ulteriori informazioni e chiarimenti, o per segnalare la volontà di non aderire a determinate iniziative o servizi del presente documento, è possibile rivolgersi al Titolare del Trattamento (o al Responsabile Interno del Trattamento) dei dati personali della scuola, indicato ai punti 2) del presente atto;

6. Modalità del trattamento:

Il trattamento dei Suoi dati personali è realizzato per mezzo delle operazioni indicate all'art. 4 n. 2) del GDPR e precisamente: raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, comunicazione, cancellazione e distruzione dei dati. I Suoi dati personali sono sottoposti a trattamento sia cartaceo che elettronico e/o automatizzato.

7. Accesso ai dati:

I Suoi dati potranno essere resi accessibili per le finalità di cui all'art. 5:

a dipendenti e collaboratori del Titolare della scuola Istituto Istruzione Superiore Scientifico e Tecnico in Italia, nella loro qualità di incaricati e/o responsabili interni del trattamento e/o amministratori di sistema.

8. Categorie di destinatari dei dati personali:

Strutture preposte all'acquisto di beni e servizi, alla liquidazione o alla gestione del contenzioso; struttura preposta al rispetto delle norme su trasparenza e anticorruzione.

9. Trasferimento dei dati in un paese extra-UE:

I dati personali sono conservati su server ubicati all'interno dell'Unione Europea. Resta in ogni caso inteso che il Titolare, ove si rendesse necessario, avrà facoltà di spostare i dati anche su server extra-UE. In tal caso, il Titolare assicura sin d'ora che il trasferimento dei dati extra-UE avverrà in conformità alle disposizioni di legge applicabili, previa stipula delle clausole contrattuali standard previste dalla Commissione Europea.

10. Periodo di conservazione dei dati:

Il periodo di conservazione dei dati può essere molto diverso; il criterio per stabilirlo si basa su principi di buon senso e sulle precisazioni dell'Autorità Garante secondo cui i

dati possono essere conservati in generale “finché sussista un interesse giustificabile” e cioè finché la loro conservazione risulti necessaria agli scopi per i quali sono stati raccolti e trattati. Più in generale, i dati dovrebbero essere conservati in linea con quanto previsto dal Codice Civile (art.2220). Il Titolare tratterà i dati personali per il tempo necessario per adempiere alle finalità di cui sopra e comunque per non oltre 5 anni dalla cessazione del rapporto per le Finalità di Servizio. I tempi di conservazione sia cartacei che telematici sono stabiliti dalla normativa di riferimento per le Istituzioni scolastiche in materia Archivistica ovvero DPR 445/2000; Decreto Legislativo 22 gennaio 2004 n. 42 Codice dei beni culturali e del paesaggio, ai sensi dell’articolo 10 della legge 6 luglio 2002, n. 137 (G.U. n. 45 del 24 febbraio 2004, s.o.n. 28).

11. Diritti dell'interessato:

Nella Sua qualità di interessato, ha i diritti di cui all’art. 7 del Codice Privacy all’art. 15 del GDPR e precisamente i diritti di:

1. ottenere la conferma dell'esistenza o meno di dati personali che La riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile;

2. ottenere l'indicazione: a) dell'origine dei dati personali; b) delle finalità e modalità del trattamento; c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici; d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'art. 3, comma 1, del GDPR; e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati

3. ottenere: a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati; b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati; c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato;

4. opporsi, in tutto o in parte: a) per motivi legittimi al trattamento dei dati personali che La riguardano, ancorché pertinenti allo scopo della raccolta; b) al trattamento di dati personali che La riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale, mediante l’uso di sistemi automatizzati di chiamata senza l’intervento di un operatore mediante e-mail e/o mediante modalità di marketing tradizionali mediante telefono e/o posta cartacea. Si fa presente che il diritto di opposizione dell’interessato, esposto al precedente punto b), per finalità di marketing diretto mediante modalità automatizzate si estende a quelle tradizionali e che comunque resta salva la possibilità per l’interessato di esercitare il diritto di opposizione anche solo in parte.

Pertanto, l’interessato può decidere di ricevere solo comunicazioni mediante modalità tradizionali ovvero solo comunicazioni automatizzate oppure nessuna delle due tipologie di comunicazione.

Ove applicabili, ha altresì i diritti di cui agli artt. 16-21 del GDPR (Diritto di rettifica, diritto all'oblio, diritto di limitazione di trattamento, diritto alla portabilità dei dati, diritto di opposizione), nonché il diritto di reclamo all'Autorità Garante.
12. Modalità di esercizio dei diritti:
Potrà in qualsiasi momento esercitare i diritti inviando:
- comunicazione tramite e-mail all'indirizzo tris009005@istruzione.it
13. Obbligo legale del conferimento dei dati e conseguenze del rifiuto di rispondere;
Il conferimento dei dati per le finalità di cui all'art. 5 A, B, C, D, E, F, G, H, I è obbligatorio. In loro assenza, non potremo garantire i servizi dell'art. 5. Il conferimento dei dati per le finalità di cui all'art. 5.J e all'art. 5.K è invece facoltativo. Può quindi decidere di non conferire alcun dato o di negare successivamente la possibilità di trattare dati già forniti. Continuerà comunque ad avere diritto ai Servizi di cui all'art. 5. A, B, C, D, E, F, G, H, I.

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.

L'istituto gode di una strumentazione tecnologica diffusa capillarmente in tutti gli spazi, grazie ai finanziamenti europei statali PON, a quelli della Regione Umbria, ai progetti del Piano Nazionale Scuola Digitale, alla Fondazione Cassa di RIsparmio di Orvieto, nonché al contributo volontario delle famiglie. La connettività è garantita dalla fibra ottica FTTC e da Wi-MAX ed offre la connessione ad internet per le attività sia didattiche sia amministrative. La LAN e la WLAN sono interfacciate a internet tramite un firewall (PfSense) che permette il bilanciamento di banda, la QoS e il filtraggio dei siti. L'assistenza tecnica del server e delle apparecchiature informatiche è gestita da una squadra di docenti esperti interni, che provvedono al controllo sul backup dei dati, all'aggiornamento dei sistemi operativi e degli antivirus installati sulle macchine e al controllo del funzionamento del firewall. La rete didattica fornisce in sicurezza la connessione alle 42 classi provviste di strumentazione tecnologica, ai laboratori informatici, scientifici, linguistici, multimediali, di disegno e storia dell'arte, alla biblioteca e alle aule multifunzionali destinate al lavoro dei docenti, per un totale di 230 PC in rete. A questi vanno aggiunti i dispositivi personali deli docenti, autenticati tramite Macaddress, utilizzati in modalità BYOD (Bring Your Own Device). L'utilizzo quotidiano del registro elettronico è gestito da Spaggiari che ne garantisce la protezione dei dati, così come la normativa richiede. Gli studenti accedono alla rete sotto il controllo dei docenti durante le attività didattiche. La sensibilizzazione rispetto all'uso delle password viene fatta attraverso la diffusione di circolari circa l'utilizzo della strumentazione tecnologica da parte dei docenti. In particolare gli assistenti tecnici informatici hanno cura di aggiornare periodicamente il software e il sistema operativo a garanzia della protezione da aggressioni esterne e dalle vulnerabilità che emergono nel tempo. L'uso della tecnologia a scuola riguarda principalmente le attività laboratoriali per cui sia i docenti sia gli studenti adottano le indicazione previste dai regolamenti approvati dal Consiglio di Istituto circa l'accesso alla Rete e ai dispositivi tecnologici. I regolamenti sono pubblicati sul sito web della scuola.

3.3 - Strumenti di comunicazione

online

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

Gli strumenti che l'Istituto adotta sono: Sito scolastico, Registro Elettronico, Mail personali e/o istituzionali.

Sito scolastico

L'istituto ha incaricato un docente interno per la redazione editoriale e la gestione delle pagine del sito della scuola https://majoranamaitani.edu.it Il Dirigente Scolastico è garante del contenuto.

La scuola detiene i diritti d'autore dei documenti che si trovano sul proprio sito o di quei documenti per i quali è stato chiesto ed ottenuto il permesso dall'autore proprietario. Le informazioni pubblicate sul sito della scuola relative alle persone da contattare rispettano le norme vigenti sulla privacy.

La scuola non pubblica sul proprio sito materiale prodotto dagli alunni senza il permesso dei loro genitori; inoltre, le fotografie degli stessi sono pubblicate previa liberatoria dei genitori o tutori.

La scuola

-utilizza il 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) per il sito web;

-utilizza un sistema di cifratura quando il trattamento di dati lo richiede (ovvero oscurare il dato per renderlo incomprensibile a coloro che non hanno i codici per accedervi, mediante la "crittografia" e, quindi, l'uso di un algoritmo di cifratura);

-sistema di backup (sistema che permette di salvare regolarmente i dati, di ripristinare eventuali file modificati o rimossi per errore dalla rete, di garantire la presenza di una copia di sicurezza di tutti i file importanti).

La scuola offre all'interno del proprio sito web i seguenti servizi alle famiglie ed agli utenti esterni:

-servizio del Registro on-line per comunicazione di voti e assenze e per prenotazione di colloqui individuali con i docenti

-segreteria digitale (pubblicazione delle circolari della Presidenza)

-consultazione elenchi libri di testo

-Piano dell'Offerta Formativa

-Regolamento di Istituto

-Patto di Corresponsabilità

-Orario delle lezioni.

Registro elettronico - Classeviva Spaggiari

Docenti

Ad ogni docente è assegnata una login e password per la gestione del registro elettronico e posta elettronica dell'Istituto.

Ogni docente firma la presenza secondo l'orario scolastico e tiene aggiornato il registro personale.

Ogni docente chiude il Registro Elettronico al termine della lezione.

Ogni docente chiude su ogni postazione la casella di posta utilizzata sia quella personale sia quella messa a disposizione dell'Istituto.

L'Istituto non risponde dell'alterazione di eventuali dati.

Studenti

Gli studenti accedono al Registro Elettronico con un profilo assegnato dal sistema, per la comunicazione sull'andamento didattico-disciplinare dell'alunno, per visualizzare le assenze, per visualizzare il lavoro svolto in classe e icompiti assegnati, per prendere atto della programmazione didattica.

Famiglie

I genitori accedono al Registro Elettronico con un profilo assegnato dal sistema, per la comunicazione sull'andamento didattico-disciplinare dell'alunno, per la prenotazione dei colloqui mattutini e pomeridiani e per prendere atto della programmazione didattica.

Dirigente, Collaboratori, Segreteria

La comunicazione formale con le famiglie avviene tramite l'invio dalle mail istituzionale della scuola alle mail personali dei genitori e/o attraverso la Bacheca del registro elettronico

3.4 - Strumentazione personale

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

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

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

Sulla base:

- del DPR 249 del 24/06/1998 " *Regolamento recante lo Statuto delle studentesse e degli studenti* ";
- del DM 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* ";
- del DM 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* ";
- della Legge 107/2015,

Si stabilisce che:

1) **L'uso dei cellulari e dei dispositivi tecnologici e di intrattenimento** da parte degli alunni, durante lo svolgimento delle attività didattiche, **è vietato, se non espressamente previsto o autorizzato dai docenti. I predetti dispositivi devono**

essere tenuti spenti e opportunamente custoditi e depositati in borsoni, zaini, giacconi, giammai possono essere tenuti dagli alunni tra le mani o sul banco**.** La violazione di tale divieto configura un'infrazione disciplinare, rispetto alla quale la scuola è tenuta ad applicare apposite sanzioni, secondo quanto previsto dalla tabella allegata nell'art. 39.

2) Durante le **verifiche scritte**, fermo quanto sancito nel punto 1), nel caso in cui lo studente sia sorpreso a utilizzare il cellulare, è possibile per i docenti ritirare o annullare la verifica.

Art. 38 USO DEI DISPOSITIVI TECNOLOGICI NELLA DIDATTICA

1) **I dispositivi tecnologici possono essere utilizzati con finalità didattiche**, in momenti ben definiti e sotto la supervisione dei docenti. In tali casi, lo smartphone (e gli altri dispositivi tecnologici, come il tablet) può essere utilizzato proficuamente nella didattica, in quanto dispone di varie funzioni (app didattiche, sistemi cloud, classi virtuali, possibilità di fare foto, video, condividere file, conferenze e altro) che possono risultare utili per lo svolgimento di attività didattiche innovative e collaborative e per l'acquisizione da parte degli alunni di un elevato livello di competenza digitale, soprattutto per quanto riguarda l'utilizzo consapevole e responsabile delle tecnologie.

2) La comunicazione con le famiglie, per qualsiasi urgenza, è sempre garantita attraverso il telefono della scuola. I docenti possono derogare a tale disposizione, consentendo l'uso del cellulare, in caso di particolari situazioni non risolvibili in altro modo.

3) Le famiglie sono invitate a collaborare strettamente con l'Istituto, nello spirito della corresponsabilità educativa, evitando ad esempio di inviare messaggi o effettuare chiamate ai telefoni dei propri figli durante l'orario scolastico.

4) Durante le uscite, visite guidate e viaggi di istruzione, l'uso è consentito, al di fuori dei momenti dedicati all'aspetto didattico delle uscite.

5) All'interno di tutti i locali della scuola, comprese palestre, aule e laboratori, sono vietate foto, riprese audio/video di ambienti e persone, salvo in caso di esplicita autorizzazione dei docenti o del Dirigente.

6) Gli studenti possono effettuare **la registrazione audio o video delle lezioni o di altre attività didattiche** , che siano in presenza o a distanza, purché abbiano preventivamente informato il docente e purché i contenuti siano usati per finalità strettamente personali e non siano oggetto di divulgazione. In nessun caso le registrazioni possono essere eseguite di nascosto, all'insaputa degli insegnanti.

7) Si ricorda che **la diffusione di contenuti audio, foto o video** è sempre subordinata al consenso da parte delle persone riprese. La diffusione non autorizzata (ad esempio online, sui vari social network) di immagini, audio o video, effettuate

all'interno degli ambienti scolastici o durante le lezioni a distanza in videoconferenza, non solo è sanzionabile dal presente regolamento, ma può anche configurare reati punibili dalla legge ed essere dunque soggetto ad eventuale denuncia presso l'autorità giudiziaria da parte degli interessati.

8) L'Istituto perseguirà, secondo l'ordinamento vigente, qualsiasi utilizzo dei social network che risulti improprio o dannoso per l'immagine e il prestigio dell'Istituto stesso, degli operatori scolastici e degli alunni. I divieti e le relative sanzioni si estendono anche a tutti i dispositivi tecnologici in possesso degli stessi.

9) Il divieto di utilizzare il cellulare per finalità estranee alla didattica è da intendersi rivolto a tutti (personale docente, non docente e alunni)

Il nostro piano d'azioni

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

Scegliere almeno 1 di queste azioni:

- Organizzare incontri per la consultazione degli studenti/studentesse suindicazioni/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
- 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.

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

Scegliere almeno 1 di queste azioni:

- 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.*

In aggiunta agli interventi già previsti in tema di cittadinanza digitale e sicurezza in rete nel curricolo digitale, l'Istituto si impegna a svolgere un'attività di prevenzione e sensibilizzazione sulle seguenti tematiche:

-Cyberbullismo

-Hate speech

-Sexting

-Adescamento online

-Pedopornografia

A tal proposito saranno privilegiati interventi esterni di associazioni e singoli esperti che trattino le suddette tematiche e sarà rafforzata e intensificata la collaborazione con le forze dell'ordine impegnate nella prevenzione dei rischi e dei reati connessi all'uso improprio della rete, attraverso un calendario di incontri con studenti e famiglie.

Nell'attività di sensibilizzazione e prevenzione sono coinvolti anche i rappresentati di Istituto degli studenti, sia attraverso attività di peer education e di sensibilizzazione, sia proponendo esperti e associazioni per lo svolgimento delle assemblee di istituto.

L'Istituto e i docenti si impegnano altresì a diffondere e promuovere tra gli studenti e le famiglie la conoscenza della piattaforma "Generazioni connesse" inserendo sul sito web istituzionale il link del progetto: www.generazioniconnesse.it, dove trovare ulteriori approfondimenti, spunti, aggiornamenti e strumenti didattici utili.

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).

VIOLAZIONI

1. Tipologie di azioni qualificate come Bullismo:

a. violenza fisica

b. violenza psicologica e intimidazione

c. isolamento della vittima

2. Tipologie qualificate come Cyberbullismo:

a. **flaming**: messaggi online violenti e volgari mirati a suscitare battaglie verbali in un forum.

b. **harassment** (molestie): spedizione ripetuta di messaggi insultanti mirati a ferire qualcuno.

c. **cyberstalking**: invio ripetuto di messaggi che includono esplicite minacce fisiche, al punto che la vittima arriva a temere per la propria incolumità.

d. **denigrazione**: pubblicazione all'interno di comunità virtuali di pettegolezzi e commenti crudeli, calunniosi e denigratori, al fine di danneggiare la reputazione della vittima

e. **esclusione**: escludere deliberatamente una persona da un gruppo online per provocare in essa un sentimento di emarginazione.

f. **outing estorto**: registrazione di confidenze creando un clima di fiducia e inserimento successivo in un contesto in rete pubblico.

g. **trickery** (inganno): ottenere la fiducia di qualcuno con l'inganno per poi pubblicare o condividere con altri le informazioni confidate via web, anche attraverso la pubblicazione di audio e video confidenziali.

h. **impersonation** (sostituzione di persona): farsi passare per un'altra persona per spedire messaggi o pubblicare testi reprensibili.

i. **sexting**: invio di messaggi via smartphone ed Internet, corredati da immagini a sfondo sessuale (reato di pedopornografia).

l. **catfishing**: è una attività ingannevole in cui la persona utilizza un account con un'identità fittizia su un social network, spesso prendendo di mira una persona per truffarla o danneggiarla o abusarne. Viene impiegato per truffe su siti di incontri.

A seguire vengono descritte le azioni previste dal PTOF 2022-2025 in relazione a questa problematica:

-presenza a scuola di referente bullismo e cyberbullismo,

-partecipazione ad eventi e incontri della Polizia Postale e/o della Polizia di Stato,

- presenza a scuola di referente dello Sportello d'ascolto, attività dello Sportello d'ascolto in presenza,

- attivazione di iniziative, di progetti e di PCTO mirati all'inclusione, all'accettazione e alla valorizzazione della diversità, al dialogo interreligioso e interculturale, alla destrutturazione degli stereoitipi, alla prevenzione della violenza di genere,

- didattica laboratoriale, inclusiva, non formale, su iniziative dei singoli docenti, mirata all'accettazione dell'altro e all'inclusione.

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.

A seguire vengono descritte le azioni previste dal PTOF 2022-2025 in relazione a questa problematica:

-presenza a scuola di referente bullismo e cyberbullismo,

-partecipazione ad eventi e incontri della Polizia Postale e/o della Polizia di Stato,

- presenza a scuola di referente dello Sportello d'ascolto, attività dello Sportello d'ascolto in presenza,

- attivazione di iniziative, di progetti e di PCTO mirati all'inclusione, all'accettazione e alla valorizzazione della diversità, al dialogo interreligioso e interculturale, alla destrutturazione degli stereoitipi, alla prevenzione della violenza di genere,

- didattica laboratoriale, inclusiva, non formale, su iniziative dei singoli docenti, mirata all'accettazione dell'altro e all'inclusione.

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?

A seguire vengono descritte le azioni previste dal PTOF 2022-2025 in relazione a questa problematica:

-presenza a scuola di referente bullismo e cyberbullismo,

-partecipazione ad eventi e incontri della Polizia Postale e/o della Polizia di Stato,

- presenza a scuola di referente dello Sportello d'ascolto, attività dello Sportello d'ascolto in presenza,

- attivazione di iniziative, di progetti e di PCTO mirati all'inclusione, all'accettazione e alla valorizzazione della diversità, al dialogo interreligioso e interculturale, alla destrutturazione degli stereoitipi, alla prevenzione della violenza di genere,

- didattica laboratoriale, inclusiva, non formale, su iniziative dei singoli docenti, mirata all'accettazione dell'altro e all'inclusione.

4.5 - Sexting

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

A seguire vengono descritte le azioni previste dal PTOF 2022-2025 in relazione a questa problematica:

-presenza a scuola di referente bullismo e cyberbullismo,

-partecipazione ad eventi e incontri della Polizia Postale e/o della Polizia di Stato,

- presenza a scuola di referente dello Sportello d'ascolto, attività dello Sportello d'ascolto in presenza,

- attivazione di iniziative, di progetti e di PCTO mirati all'inclusione, all'accettazione e alla valorizzazione della diversità, al dialogo interreligioso e interculturale, alla destrutturazione degli stereoitipi, alla prevenzione della violenza di genere,

- didattica laboratoriale, inclusiva, non formale, su iniziative dei singoli docenti, mirata all'accettazione dell'altro e all'inclusione.

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.

A seguire vengono descritte le azioni previste dal PTOF 2022-2025 in relazione a questa problematica:

-presenza a scuola di referente bullismo e cyberbullismo,

-partecipazione ad eventi e incontri della Polizia Postale e/o della Polizia di Stato,

- presenza a scuola di referente dello Sportello d'ascolto, attività dello Sportello d'ascolto in presenza,

- attivazione di iniziative, di progetti e di PCTO mirati all'inclusione, all'accettazione e alla valorizzazione della diversità, al dialogo interreligioso e interculturale, alla destrutturazione degli stereoitipi, alla prevenzione della violenza di genere,

- didattica laboratoriale, inclusiva, non formale, su iniziative dei singoli docenti, mirata all'accettazione dell'altro e all'inclusione.

4.7 - Pedopornografia

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

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

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

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

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

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

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

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2022/2023).

Scegliere almeno 1 di queste azioni:

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

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

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

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

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

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

Scegliere almeno 1 di queste azioni:

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

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

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

Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

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

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

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

Nelle procedure:

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

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

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

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

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

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

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

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

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

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

Vi suggeriamo, inoltre, i seguenti servizi:

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

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

segnalare la presenza di materiale pedopornografico online.

In riferimento ai reati digitali e nell'espletamento del suo dovere di vigilanza, il docente potrebbe trovarsi di fronte al caso in cui sospetta 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 oppure ha evidenza certa che stia accadendo qualcosa tra gli/le studenti/esse della propria classe.

Nel CASO SOSPETTO il docente coinvolge innanzitutto il referente d'Istituto per il contrasto del bullismo e del cyberbullismo (ed eventualmente anche il gruppo di ePolicy) valutando insieme le possibili strategie d'intervento. A seconda della portata dell'accaduto, il docente può inoltre avvisare l'intero consiglio di classe e, se si ravvisa la necessità, coinvolgere il Dirigente Scolastico. Nel frattempo, il docente e i docenti informati ascoltano gli studenti e le studentesse, osservando e monitorando il clima di classe, ciò che accade e le dinamiche relazionali nel contesto classe, senza fare indagini dirette.

Nel CASO EVIDENTE, il docente condivide immediatamente quanto osservato con il referente per il bullismo e il cyberbullismo, (ed eventualmente anche il gruppo di ePolicy), valutando insieme le possibili strategie di intervento. Si avvisa anche il Dirigente Scolastico che convoca il consiglio di classe. Se non si ravvisano fattispecie di reato, si procede nel seguente modo:

-si informano i genitori (o chi esercita la responsabilità genitoriale) degli/delle studenti/studentesse direttamente coinvolti/e (qualsiasi ruolo abbiano avuto) su quanto accaduto e si condividono informazioni e strategie;

-si richiede, se possibile e se presente nell'Istituto, la consulenza dello psicologo scolastico a supporto della gestione della situazione, in base alla gravità dell'accaduto;

-si informare i genitori degli/delle studenti/studentesse infra quattordicenni della possibilità di richiedere la rimozione, l'oscuramento o il blocco di contenuti offensivi ai gestori di siti internet o social (o successivamente, in caso di non risposta, al garante della Privacy);

-si informano gli/le studenti/studentesse ultra quattordicenni della possibilità di richiedere la rimozione, l'oscuramento o il blocco di contenuti offensivi ai gestori di siti internet o social (o successivamente, in caso di non risposta, al garante della Privacy);

-si attiva il consiglio di classe;

A seconda della situazione e delle valutazioni effettuate con referente, dirigente e genitori, si valuta la segnalazione alla Polizia Postale delle seguenti informazioni:

a) contenuto del materiale online offensivo

b) modalità di diffusione

c) fattispecie di reato eventuale

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.

COMPITI DELLE FIGURE COINVOLTE

1. **Dirigente Scolastico**

In base all'art. 5 comma 1 della LEGGE 29 maggio 2017, n. 71 "Salvo che il fatto costituisca reato, in applicazione della normativa vigente e delle disposizioni di cui al comma 2, il dirigente scolastico che venga a conoscenza di atti di cyberbullismo ne informa tempestivamente i soggetti esercenti la responsabilità genitoriale ovvero i tutori dei minori coinvolti e attiva adeguate azioni di carattere educativo".

In base alla Direttiva MIUR "*Aggiornamento linee di orientamento per la prevenzione e il contrasto del cyberbullismo*", Ottobre 2017, il Dirigente scolastico:

a. individua attraverso il Collegio dei Docenti un **referente** del bullismo e cyberbullismo;

b. coinvolge, nella prevenzione e contrasto al fenomeno del bullismo, tutte le componenti della comunità scolastica, particolarmente quelle che operano nell'area dell'informatica, partendo dall'utilizzo sicuro di Internet a scuola;

c. prevede all'interno del PTOF corsi di aggiornamenti e formazione in materia di prevenzione dei fenomeni di bullismo e cyberbullismo, rivolti al personale docente e non docente;

d. promuove sistematicamente azioni di sensibilizzazione dei fenomeni del bullismo e cyberbullismo nel territorio in rete con enti, associazioni, istituzioni locali ed altre scuole, coinvolgendo alunni, docenti, genitori ed esperti;

e. favorisce la discussione all'interno della scuola, attraverso i vari organi collegiali, creando i presupposti di regole condivise di comportamento per il contrasto e prevenzione dei fenomeni del bullismo e cyberbullismo;

f. prevede azioni culturali ed educative rivolte agli studenti, per acquisire le competenze necessarie all'esercizio di una cittadinanza digitale consapevole.

2. **Referente "Bullismo e Cyberbullismo"**

a. promuove la conoscenza e la consapevolezza del bullismo e del cyberbullismo attraverso progetti d'istituto che coinvolgano studenti, genitori e tutto il personale;

b. monitora e presta particolare attenzione ai diversi fenomeni che si possono venire a creare all'interno della scuola;

c. promuove la costituzione di un gruppo di lavoro allargato per il supporto agli

studenti sui temi del bullismo e del cyberbullismo;

d. comunica con partner esterni alla scuola, quali servizi sociali e sanitari, aziende del privato sociale, forze di polizia, etc. per realizzare un progetto di prevenzione;

e. cura l'organizzazione e la diffusione di eventuali convegni/seminari/corsi e della giornata mondiale sulla Sicurezza in Internet la "Safer Internet Day";

f. cura, insieme al DS, la comunicazione interna: diffusione di iniziative: bandi, attività concordate con enti esterni, coordinamento delle attività finalizzate a sensibilizzare circa il fenomeno del bullismo e cyberbullismo;

g. cura, insieme al DS, la costituzione di uno spazio dedicato sul sito;

h. raccoglie e diffonde documentazione e buone pratiche;

i. promuove lo "star bene a scuola" e l'uso di metodologie didattiche innovative;

j. partecipa ad iniziative promosse dal MIUR/USR nell'ambito del bullismo e del cyberbullismo.

3. **Collegio dei Docenti**

a. promuove scelte didattiche ed educative, anche in collaborazione con altre scuole in rete, per la prevenzione del fenomeno.

4. **Consiglio di classe**

a. pianifica attività didattiche e/o integrative finalizzate al coinvolgimento attivo e collaborativo degli studenti e all'approfondimento di tematiche che favoriscano la riflessione sulla necessità dei valori di convivenza civile;

b. favorisce un clima collaborativo all'interno della classe e nelle relazioni con le famiglie propone progetti di educazione alla legalità e alla cittadinanza attiva;

c. interviene, per quanto di competenza, nei casi di bullismo e cyberbullismo che riguardano gli studenti della classe.

d. i docenti del consiglio favoriscono una relazione di fiducia con gli alunni in modo da facilitare la comunicazione di situazioni problematiche relative al bullismo e al cyberbullismo.

5. **Genitori**

a. partecipano attivamente alle azioni di formazione/informazione, istituite dalle scuole, sui comportamenti sintomatici del bullismo e del cyberbullismo;

b. sono attenti ai comportamenti dei propri figli;

c. vigilano sull'uso delle tecnologie da parte dei ragazzi controllando più possibile il contenuto degli interventi dei propri figli sui Social Network;

d. conoscono le azioni messe in campo dalla scuola e collaborano secondo le modalità previste dal Patto di Corresponsabilità;

e. conoscono il regolamento di Istituto;

f. conoscono le sanzioni previste dal regolamento d'istituto nei casi di bullismo, cyberbullismo e navigazione on-line a rischio.

7. **Studentesse e studenti**

a. sono coinvolti nella progettazione e nella realizzazione delle iniziative scolastiche, al fine di favorire un miglioramento del clima relazionale; in particolare, dopo opportuna formazione, possono operare come tutor per altri studenti (progetto Peer);

b. imparano le regole basilari, per rispettare gli altri, quando sono connessi alla rete, facendo attenzione alle comunicazioni (email, sms, wa) che inviano.

L'indirizzo mail e il nome del referente a cui sarà possibile rivolgersi per inoltrare segnalazioni, sarà disponibile sul sito web dell'Istituto nella sezione "ePolicy: uso corretto e consapevole della rete a scuola"

5.3. - Gli attori sul territorio

Talvolta, nella gestione dei casi, può essere necessario rivolgersi **ad altre figure, enti, istituzioni e servizi presenti sul territorio** qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.

Per una mappatura degli indirizzi di tali strutture è possibile consultare il Vademecum di Generazioni Connesse "Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all'utilizzo delle tecnologie digitali da parte dei più giovani" (seconda parte, pag. 31), senza dimenticare che la Helpline di Telefono Azzurro (19696) è sempre attiva nell'offrire una guida competente ed un supporto in tale percorso.

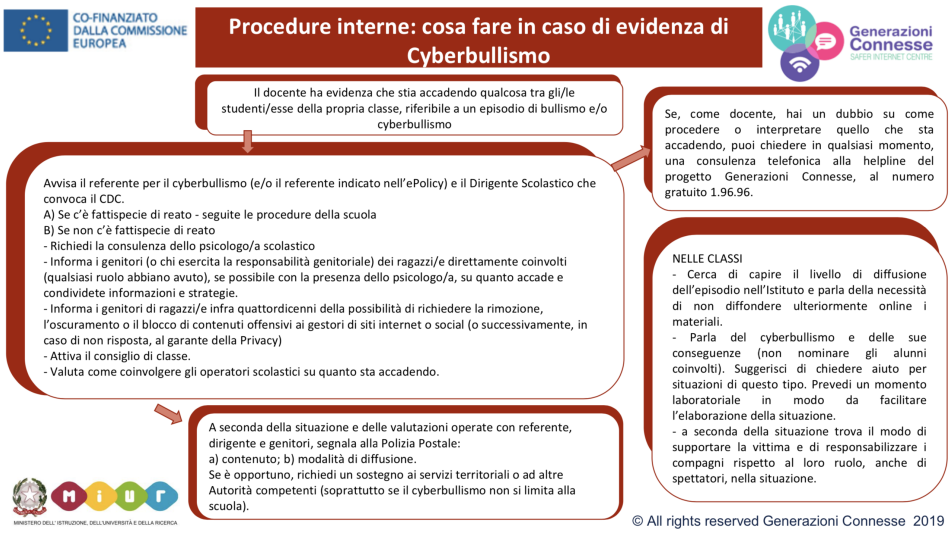
A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all'utilizzo di Internet può presentare.

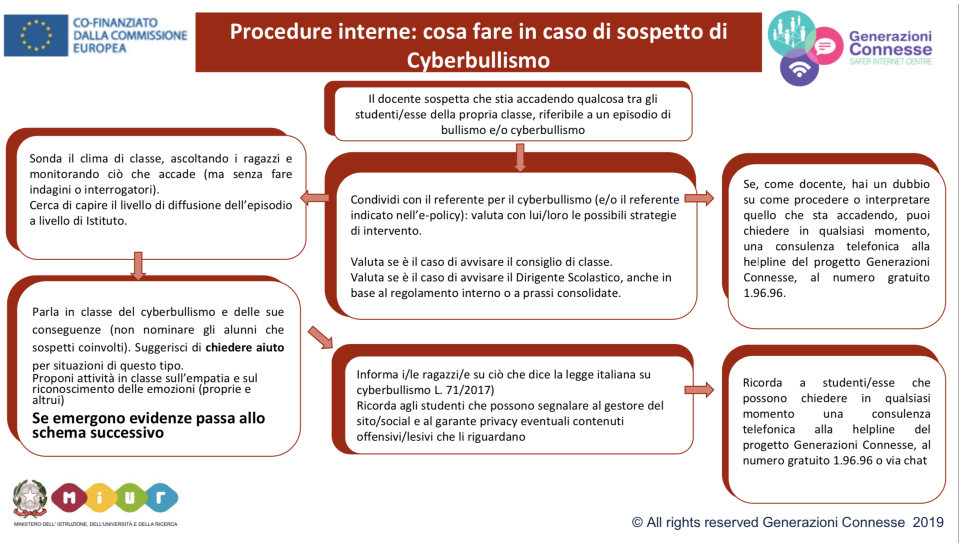
- **Comitato Regionale Unicef**: laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.

- **Co.Re.Com. (Comitato Regionale per le Comunicazioni)**: svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare attenzione alla tutela dei minori.
- **Ufficio Scolastico Regionale**: supporta le scuole in attività di prevenzione ed anche nella segnalazione di comportamenti a rischio correlati all'uso di Internet.
- **Polizia Postale e delle Comunicazioni**: accoglie tutte le segnalazioni relative a comportamenti a rischio nell'utilizzo della Rete e che includono gli estremi del reato.
- **Aziende Sanitarie Locali**: forniscono supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in Rete. In alcune regioni, come il Lazio e la Lombardia, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da Internet e alle situazioni di rischio correlate.
- **Garante Regionale per l'Infanzia e l'Adolescenza e Difensore Civico**: segnalano all'Autorità Giudiziaria e ai Servizi Sociali competenti; accolgono le segnalazioni di presunti abusi e forniscono informazioni sulle modalità di tutela e di esercizio dei diritti dei minori vittime. Segnalano alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.
- **Tribunale per i Minorenni**: segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

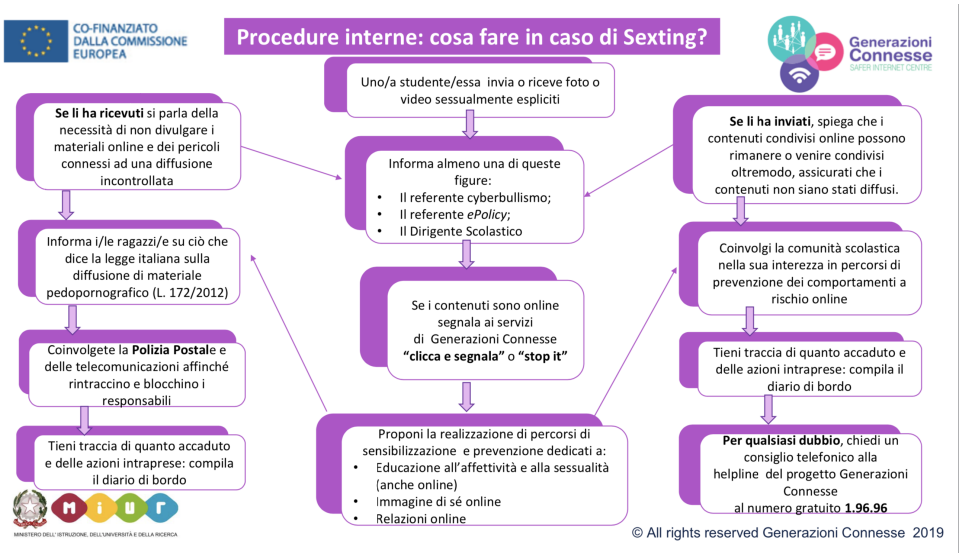
5.4. - Allegati con le procedure

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

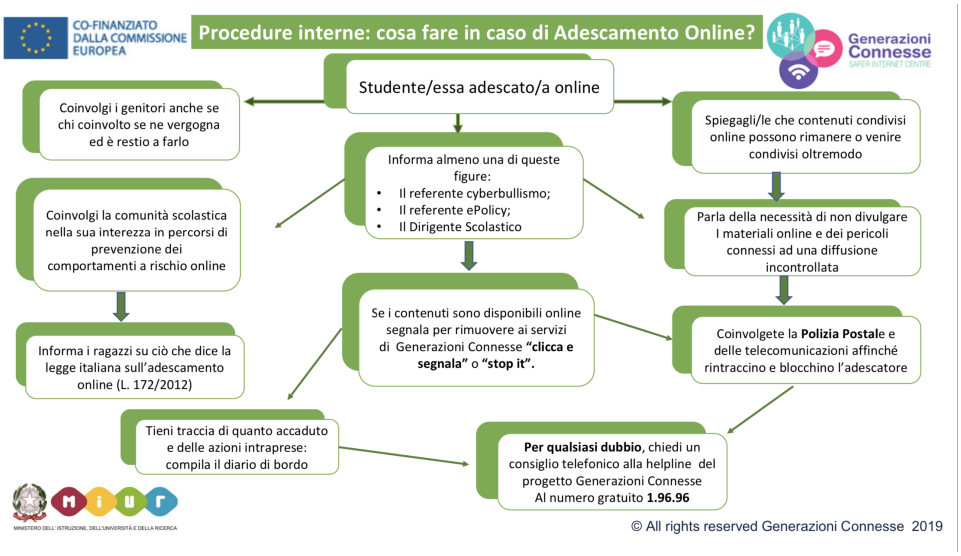




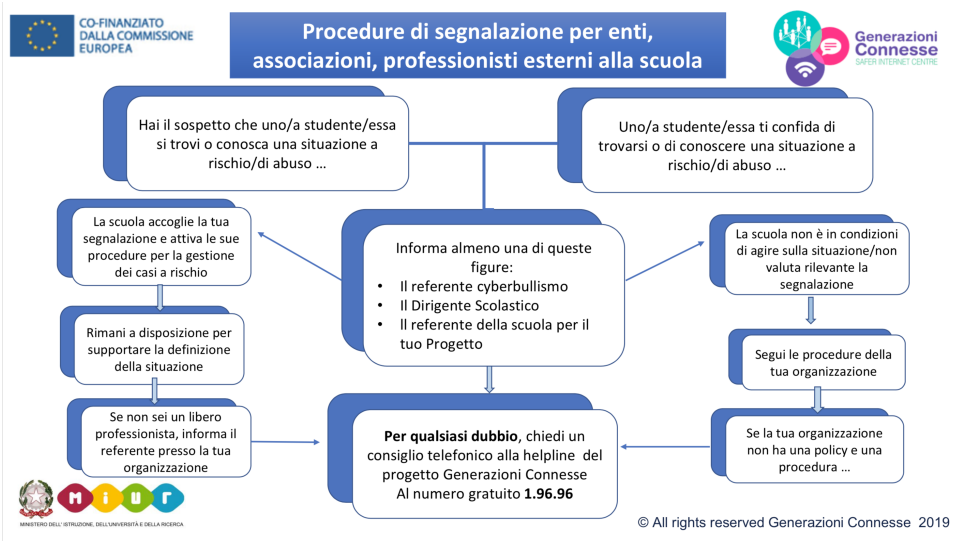
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



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



Altri allegati

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

INTERVENTI DISCIPLINARI

1. **Prima fase**: analisi e valutazione dei fatti a cura del coordinatore di classe/insegnante della classe.

Coinvolgimento del referente bullismo/cyberbullismo ed eventuali altri educatori.

Raccolta di informazioni sull'accaduto: interviste e colloqui con i singoli e con il gruppo; raccolta delle diverse versioni e ricostruzione dei fatti e dei punti di vista. In questa fase *è* importante astenersi dal formulare giudizi; è piuttosto necessario creare un clima di empatia, di solidarietà e di disponibilità al confronto che permetta un'oggettiva raccolta di informazioni. L'insegnante è un mediatore in un contesto neutro.

Raccolta di prove e documenti: quando è successo, dove, con quali modalità.

Comunicazione al Dirigente Scolastico (verbalmente e in forma scritta).

2. **Seconda fase:** risultati sui fatti oggetto di indagine e tentativo di conciliazione.

In questa fase si possono verificare due possibilità:

a. i fatti non sono configurabili come bullismo e cyberbullismo e non si ritiene di intervenire in modo specifico. Si prosegue comunque il compito educativo attraverso gli interventi mirati elencati in tabella.

b. dall'esame dei fatti e delle prove oggettive emergono elementi di un'azione vessatoria. Allora si apre un protocollo con uso di apposita modulistica e vengono stabilite le azioni da intraprendere privilegiando sanzioni disciplinari di tipo riparativo anche convertibili in attività in favore della comunità scolastica.

3. **Terza fase:** azioni e provvedimenti

INTERVENTI EDUCATIVI (caso a.)		**MISURE DISCIPLINARI** (caso b.)	
SOGGETTI COINVOLTI	Referente Docenti Studentesse/i Genitori	**SOGGETTI COINVOLTI**	Dirigente Docenti Studentesse/i Genitori

AZIONI

- Incontri con gli alunni coinvolti e loro responsabilizzazione rispetto all'accaduto
- Interventi di discussione in classe

AZIONI

- Convocazione della famiglia
- Convocazione del Consiglio di Classe
- Eventuali sanzioni previste come da art. 25 del presente regolamento
- Lettera di scuse alla vittima da parte del responsabile
- Attività a favore della comunità scolastica

Il nostro piano d'azioni

Ridefinizione del Regolamento d'Istituto nell'ottica dell'E-Policy.

Creazione sul sito di una sezione dedicata alle procedure di segnalazione di violazione e alla modulistica specifica, con indicazione dei principali Enti e Servizi a cui rivolgersi per assistenza e tutela.