



Documento di ePolicy SC. SEC I GRADO "G. FLOREANINI"

VIA TERRACINI N. 23 - 28845 - DOMODOSSOLA

Verbano-Cusio-Ossola (VB) - Piemonte

Data di approvazione: 18/06/2025 - 11:44

Cap 1 - Lo scopo della ePolicy

1.1 Scopo della ePolicy

Capitolo 1 - Presentazione dell'ePolicy

1. Scopo dell'ePolicy
2. Ruoli e responsabilità nell'implementazione dell'ePolicy
3. Integrazione dell'ePolicy con regolamenti e normativa generale esistenti
4. Condivisione e comunicazione dell'ePolicy all'intera comunità educante
5. I piani di Azione dell'ePolicy

Capitolo 2 - Sensibilizzazione e prevenzione

1. Sensibilizzazione e prevenzione
2. Il Curricolo Digitale
3. IL KIT DIDATTICO

Capitolo 3 - Gestione dell'infrastruttura e della strumentazione ICT (Information and Communication Technology) della e nella scuola

1. Protezione dei dati personali e GDPR
2. Accesso ad Internet
3. Strumenti di comunicazione online (PUA)
4. Strumentazione personale (BYOD)

Capitolo 4 - Segnalazione e gestione dei casi

1. Cosa segnalare
2. Come segnalare: quali strumenti e a chi
3. Gli attori sul territorio per intervenire
4. Allegati con le procedure

1.1 Scopo dell'ePolicy

(Questo paragrafo illustra lo scopo e gli obiettivi di questo documento programmatico per la cittadinanza digitale)

L' E-Policy ha come obiettivo principale quello di promuovere le competenze digitali per un uso delle tecnologie digitali positivo, critico e consapevole, da parte degli studenti e delle studentesse guidati dagli adulti coinvolti nel processo didattico-educativo.

La competenza digitale è una competenza chiave del cittadino europeo come indicato dal Consiglio Europeo

(Raccomandazione del 2018) che permette ad ogni cittadino di esercitare i propri diritti all'interno degli ambienti digitali (ONU - [Commento Generale 25](#): I diritti dei minori negli ambienti digitali).

L'ePolicy è un documento programmatico che permette di lavorare su quattro obiettivi:

1. Il piano di azioni triennale per promuovere nell'intera comunità scolastica l'uso sicuro responsabile e positivo della rete;
2. le misure per la prevenzione e la sensibilizzazione di comportamenti on-line a rischio;
3. le norme comportamentali e le procedure di utilizzo delle Tecnologie dell'Informazione e della Comunicazione (ICT) in ambiente scolastico;
4. le misure per la rilevazione, segnalazione e gestione delle situazioni rischiose legate ad un uso non corretto delle tecnologie digitali.

Le competenze digitali per il lavoro e per la vita sono al vertice dell'agenda politica europea. Il quadro di riferimento DigComp crea una visione condivisa di ciò che è necessario in termini di competenze per superare le sfide che derivano dalla digitalizzazione in quasi tutti gli aspetti della vita moderna.

Il modello concettuale di riferimento del DigComp 2.2 costituisce il punto di riferimento fondamentale per lo sviluppo delle 21 competenze da esso delineate.



L'11 maggio 2022 è stata adottata una [nuova strategia](#) europea (BIK+) con la finalità di garantire la protezione e il rispetto dei minori, sviluppando il loro senso di responsabilità rispetto al mondo online.

BIK+ propone delle azioni incentrate su tre pilastri:

1. **Esperienze digitali sicure** - proteggere i minori da contenuti, comportamenti e rischi online dannosi e illegali. L'obiettivo è migliorare il benessere dei giovani consumatori online attraverso un ambiente digitale sicuro e adeguato all'età, creato in modo da rispettare l'interesse superiore dei minori.
2. **Responsabilizzazione digitale** - consentire a tutti i minori (compresi quelli in situazioni di vulnerabilità) di acquisire le capacità e le competenze necessarie per compiere scelte valide ed esprimersi online in modo sicuro e responsabile
3. **Partecipazione attiva** - rispetto dei minori, dando loro voce in capitolo nell'ambiente digitale: maggior numero di attività guidate dai minori per promuovere esperienze digitali sicure, innovative e creative.

L'intento della scuola, alla luce del DigComp e di BIK+, è quello di:

- promuovere l'uso consapevole e critico da parte degli/le studenti/esse delle tecnologie digitali e di internet;
- promuovere l'acquisizione delle procedure e delle competenze "tecniche" e delle corrette norme comportamentali;
- prevenire, rilevare e fronteggiare le problematiche che derivano da un utilizzo non responsabile, pericoloso o dannoso, delle tecnologie digitali.

Gli utenti, soprattutto i minori, devono essere pienamente consapevoli dei rischi a cui si espongono quando navigano in rete. Durante il lavoro online è possibile entrare accidentalmente in contatto con materiale inadeguato e/o illegale, pertanto la scuola promuove l'adozione di strategie che limitino l'accesso a siti e/o applicazioni illegali.

Gli insegnanti hanno la responsabilità di guidare gli studenti nelle attività online a scuola e di indicare regole di condotta chiare per un uso critico e consapevole di Internet anche a casa, con la finalità di prevenire il verificarsi di situazioni potenzialmente pericolose.

Contenuti che la scuola intende affrontare con gli studenti e le studentesse nell'arco dei tre anni della scuola media, attraverso una metodologia trasversale che coinvolge tutti i docenti delle varie discipline:

- **Educare all'informazione:** il funzionamento dei motori di ricerca e i siti didattici; la valutazione dell'attendibilità e l'aggiornamento di un sito; la creazione di cartelle e sottocartelle, l'organizzazione e la classificazione dei contenuti digitali; la proprietà intellettuale e i diritti di autore per lavorare con la musica, le immagini e i testi reperibili in internet.
- **Cultura e creatività digitale:** la rielaborazione delle informazioni (no al plagio); la citazione delle fonti; la creazione di un link e di una sitografia; la collaborazione a un file condiviso (cooperative learning e peer to peer); la creazione di presentazioni, di fogli di calcolo; la conoscenza e l'uso di web-app, ecc.; il Social reading; la creazione di un video, di un podcast; il Coding e il pensiero computazionale.
- **Educazione ai media:** la conoscenza dei rischi della rete; gli elementi normativi sulla tutela della privacy; la

normativa di base sull'utilizzo dei social network; l'approfondimento dei concetti di netiquette, flame, tag; la protezione dei dati personali e della propria immagine (no alla loro diffusione, no all'iscrizione on-line senza la presenza di un genitore)

Attenzione e responsabilizzazione di tutti i docenti e di tutti gli adulti di riferimento rispetto alle aree di rischio:

- utilizzo non corretto della strumentazione della scuola;
- utilizzo del cellulare nonostante il divieto;
- mancata considerazione dei diritti d'autore relativamente a musica e film;
- controllo dell'autenticità e dell'esattezza dei contenuti online;
- cyberbullismo;
- privacy: divulgazione di informazioni personali e/o pubblicazione di foto o immagini non autorizzate e/o compromettenti;
- salute e benessere (quantità di tempo speso online su Internet o giochi)

Attività progettuali:

- patente di smartphone per le classi prime (prevenzione universale);
- incontri con le Forze dell'ordine sui rischi del mondo online per studentesse, studenti, famiglie (prevenzione universale);
- Save the Children: incontri con i volontari sui rischi del web;
- #sbullizziamoci per le classi seconde: peer to peer con studenti e studentesse della scuola secondaria di secondo grado (prevenzione universale)
- Sportello di ascolto gestito da un esperto esterno per tutta la comunità scolastica (prevenzione universale, indicata, selettiva)
- interventi di prevenzione nelle classi da parte del referente del cyberbullismo in sinergia con l'esperto esterno (prevenzione universale e selettiva);

- segnalazione da parte della comunità scolastica (docenti, personale scolastico, studenti e studentesse, famiglie) al referente del cyberbullismo di eventuali comportamenti a rischio degli alunni; interventi nelle classi e predisposizione di attività mirate (prevenzione selettiva);
- spettacoli/conferenze sul tema proposti da enti esterni.

1.2 - ePolicy: ruoli e responsabilità nell'implementazione dell'ePolicy

- (In questo paragrafo vengono dettagliati ruoli e responsabilità nell'implementazione del documento all'interno dei contesti scolastici ivi inclusi rappresentanti genitori e studenti per secondaria II grado).

Affinché l'ePolicy 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.

È opportuno che nel documento vengano definiti con chiarezza ruoli, compiti e responsabilità di ciascuna delle figure all'interno dell'Istituto.

In questo paragrafo dell'ePolicy è importante specificare le figure professionali che, a vario titolo, si occupano di gestione e programmazione delle attività formative, didattiche ed educative dell'Istituto e tutte quelle figure appartenenti alla comunità educante.

IL DIRIGENTE SCOLASTICO

Il ruolo del Dirigente Scolastico nel promuovere l'uso consentito delle tecnologie digitali e di internet include i seguenti compiti:

- promuovere la cultura della sicurezza online e garantirla a tutti i membri della comunità scolastica, in linea con il quadro normativo di riferimento, le indicazioni del MIM, delle sue agenzie e attraverso il documento di ePolicy;
- promuovere la cultura della sicurezza online – anche attraverso il documento di ePolicy - integrandola ed inserendola nelle misure di sicurezza più generali dell'intero Istituto;
- ha la responsabilità di fornire sistemi per un uso sicuro delle TIC, internet, i suoi strumenti ed ambienti e deve garantire alla popolazione scolastica la sicurezza di navigazione tramite internet utilizzando adeguati sistemi informatici e filtri;
- ha la responsabilità della gestione dei dati e della sicurezza delle informazioni e garantisce che l'Istituto segue le pratiche migliori possibili nella gestione dei dati stessi;
- deve tutelare la scuola e garantire agli utenti la sicurezza di navigazione utilizzando adeguati sistemi informatici e servizi di filtri Internet;
- ha il compito di garantire a tutto il personale una formazione adeguata sulla sicurezza online per essere tutelato nell'esercizio del proprio ruolo educativo e non;
- deve essere a conoscenza delle procedure da seguire in caso di un grave incidente di sicurezza online;

- deve garantire adeguate valutazioni di rischio nell'usare strumenti e TIC, effettuate in modo che comunque quanto programmato possa soddisfare le istanze educative e didattiche dichiarate nel PTOF di Istituto;
- deve garantire l'esistenza di un sistema che assicuri il monitoraggio e il controllo interno della sicurezza online in collaborazione con le figure di sistema;
- deve essere a conoscenza ed attuare le procedure necessarie in caso di grave incidente di sicurezza online.

L'ANIMATORE DIGITALE E IL TEAM PER L'INNOVAZIONE DIGITALE

L'animatore digitale e il Team per l'Innovazione digitale sono co-responsabili, con il referente ePolicy, dell'attuazione dei piani di azione in particolare in riferimento alla formazione dei docenti. Sono inoltre responsabili del controllo all'accesso da parte degli studenti delle Tic

IL REFERENTE PER IL BULLISMO E CYBERBULLISMO

Il referente cyberbullismo è co-responsabile, con il team ePolicy, dell'attuazione dei piani di azione e coordina le iniziative di prevenzione e contrasto del cyberbullismo.

IL TEAM ANTIBULLISMO E PER L'EMERGENZA

In coerenza con le Linee di Orientamento per la prevenzione e il contrasto del Bullismo e Cyberbullismo del Ministero dell'Istruzione (D.M. n. 18 del 13/1/2021, agg. 2021 - nota prot. 482 del 18-02-2021), il Team ha le funzioni di coadiuvare il Dirigente Scolastico, coordinatore del Team nella scuola, nella definizione degli interventi di prevenzione e nella gestione dei casi di bullismo e cyberbullismo che si possono presentare. Promuove inoltre la conoscenza e la consapevolezza del bullismo e del cyberbullismo attraverso progetti d'istituto che coinvolgano genitori, studenti e tutto il personale e comunica ad alunni, famiglie e tutto il personale scolastico dell'esistenza del team, a cui poter fare riferimento per segnalazioni o richieste di informazioni sul tema.

Il Team ha il compito di:

- coadiuvare il Dirigente scolastico, coordinatore del Team, nella definizione degli interventi di prevenzione del bullismo (per questa funzione partecipano anche il presidente del Consiglio d'Istituto e i Rappresentanti degli studenti).
- Intervenire (come gruppo ristretto, composto da Dirigente e referente o referenti per il bullismo e il cyberbullismo, psicologo o pedagogo, se presente) nelle situazioni acute di bullismo.
- Promuovere la redazione e l'applicazione della ePolicy e monitorare le segnalazioni.

I/LE DOCENTI

I/le docenti hanno un ruolo centrale nel diffondere la cultura dell'uso responsabile delle TIC e della Rete. Possono, innanzitutto, integrare la propria disciplina con approfondimenti, promuovendo l'uso delle tecnologie digitali nella didattica. I docenti devono accompagnare e supportare gli/le studenti nelle attività di apprendimento e nei laboratori che prevedono l'uso della LIM o di altri dispositivi tecnologici che si connettono alla Rete. Inoltre, educano gli studenti alla prudenza, a non fornire dati ed informazioni personali, ad abbandonare un sito dai contenuti che possono turbare o spaventare e a non incontrare persone conosciute in Rete senza averne prima parlato con i genitori. Informano gli alunni sui rischi presenti in

Rete, senza demonizzarla, ma sollecitandone un uso consapevole, in modo che Internet possa rimanere per bambini/e e ragazzi/e una fonte di divertimento e uno strumento di apprendimento.

I/le docenti osservano altresì regolarmente i comportamenti a rischio (sia dei potenziali bulli, sia delle potenziali vittime) e hanno il dovere morale e professionale di segnalare al Dirigente Scolastico qualunque problematica, violazione o abuso, anche online, che veda coinvolti studenti e studentesse dandone tempestiva comunicazione al Dirigente Scolastico, al Referente per il Cyberbullismo e Bullismo e al Consiglio di Classe per definire strategie di intervento condivise.

RESPONSABILE DELLA PROTEZIONE DEI DATI

Il Responsabile della protezione dei dati (RPD o DPO) conosce l'ePolicy di Istituto, fornisce la propria consulenza in merito agli obblighi derivanti dal GDPR e sorveglia sull'esatta osservanza della normativa in materia di tutela dei dati personali ed è co-responsabile delle azioni di informazione e formazione nell'Istituto sulla protezione dei dati personali

IL PERSONALE AMMINISTRATIVO, TECNICO E AUSILIARIO (ATA)

Il personale ATA, all'interno dei singoli regolamenti d'Istituto, è coinvolto nelle pratiche di prevenzione - ivi incluso il processo di definizione e implementazione dell'ePolicy di Istituto - ed è tenuto alla segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo.

GLI STUDENTI E LE STUDENTESSE

Gli studenti e le studentesse devono, in relazione al proprio grado di maturità e consapevolezza raggiunta, utilizzare al meglio le tecnologie digitali in coerenza con quanto richiesto dai docenti. Con il supporto della scuola dovrebbero imparare a tutelarsi online, tutelare i/le propri/e compagni/e e rispettarli/le. Affinché questo accada devono partecipare attivamente a progetti ed attività che riguardano l'uso positivo delle TIC e della Rete e farsi promotori di quanto appreso anche attraverso possibili percorsi di peer education.

I rappresentanti degli/delle studenti sono informati del documento di ePolicy e invitati a costruire i piani di azione, a partire dal secondo anno della secondaria di II grado,

I GENITORI/ADULTI DI RIFERIMENTO

I Genitori, in continuità con l'Istituto scolastico, sono attori partecipi e attivi nelle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete, nonché sull'uso responsabile degli strumenti personali (pc, smartphone, etc). Come parte della comunità educante sono tenuti a relazionarsi in modo costruttivo con i/le docenti sulle linee educative che riguardano le TIC e la Rete e - ivi incluso il documento di ePolicy - comunicare con loro circa i problemi rilevati quando i/le propri/e figli/e non usano responsabilmente le tecnologie digitali o Internet.

È estremamente importante che accettino e condividano quanto scritto nell'ePolicy d'Istituto e nel patto di corresponsabilità in un'ottica di collaborazione reciproca. Si promuove il coinvolgimento dei rappresentanti di genitori/adulti di riferimento all'interno del percorso di definizione e implementazione dell'ePolicy.

GLI ENTI ESTERNI PUBBLICI E PRIVATI E LE ASSOCIAZIONI

Enti esterni pubblici e privati, il mondo dell'associazionismo dovranno conformarsi alla politica della scuola riguardo all'uso consapevole delle TIC e della rete per la realizzazione di iniziative nelle scuole, finalizzate a promuovere un uso positivo e consapevole delle Tecnologie Digitali da parte dei più giovani, e/o finalizzate a prevenire e contrastare situazioni di rischio online e valutare la rispondenza delle proposte di attività di sensibilizzazione/formazione alle esigenze di qualità contenute nel documento di ePolicy. Dovranno inoltre promuovere comportamenti sicuri durante le attività che si svolgono con gli/le studenti e verificare di aver implementato una serie di misure volte a garantire la tutela dei minori nel caso di insorgenza di problematiche e ad assicurarne la tempestiva individuazione e presa in carico.

Azioni dell'Animatore digitale

- Effettua una rilevazione del fabbisogno formativo dei docenti sui temi dell'educazione civica digitale, utilizzando, se ritenuto necessario, SELFIE FOR TEACHERS, lo strumento di autoriflessione sulle competenze digitali degli insegnanti di ogni ordine e grado, proposto gratuitamente dalla Commissione Europea sulle indicazioni del DigCompEdu, il framework delle competenze europee del docente/formatore; utilizza anche il questionario SELFIE proposto dalla Commissione Europea, che aiuta a comprendere il livello di utilizzo positivo del digitale nell'Istituto.
- Stimola la formazione interna all'istituzione negli ambiti di utilizzo della piattaforma scolastica (per esempio Google Suite).
- Fornisce consulenza e informazioni, insieme al gruppo di lavoro del team digitale, al personale rispetto ai rischi online e alle misure di prevenzione e gestione degli stessi.
- Monitora e rileva le problematiche emergenti, relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola, in coordinamento con il team digitale e, se necessario, con il DPO.
- Propone la revisione delle politiche dell'istituzione, con l'individuazione di soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola.
- Si attiva perché gli utenti possano accedere alla rete della scuola tramite dispositivi scolastici e account scolastici personali, regolarmente gestiti dal team digitale attraverso la piattaforma di amministrazione.

Azioni del Referente al cyberbullismo

- supporta il Dirigente scolastico nella revisione/stesura di Regolamenti (Regolamento d'istituto), atti e documenti (PTOF, PdM, Rav);
- coordina le iniziative di prevenzione e contrasto al cyberbullismo. A tal fine, si avvale anche della collaborazione delle Forze dell'ordine e delle Associazioni del territorio;
- assicura che l'educazione alla sicurezza online sia incorporata in tutto il programma di studi;
- promuove la consapevolezza e l'impegno per la salvaguardia online in tutta la comunità scolastica;

- promuove la formazione e dà consulenza a tutto il personale;
- promuove attività o progetti da svolgere nelle classi;
- applica e controlla i protocolli di rilevazione, monitoraggio e gestione delle potenziali azioni di cyber bullismo;
- diffonde la E- Safety Policy attraverso power point e schede semplificative;
- collabora con tutte le agenzie educative e istituzionali (Associazioni, Polizia postale, Forze dell'ordine, etc.) per prevenire e gestire i casi di possibile cyber bullismo;
- coinvolge la comunità scolastica (alunni, genitori e altri attori del territorio) nella partecipazione ad attività e progetti attinenti l'utilizzo consapevole di internet.

Azioni del Team antibullismo

- Calendarizza riunioni trimestrali che prevedono il coinvolgimento del D.S., del Referente Cyberbullismo, del DPO, dell'Animatore Digitale, per verificare eventuali esigenze specifiche dell'istituto e condividere i risultati relativi alle azioni svolte.
- Mette a disposizione della comunità educante un modulo di prima segnalazione (sul proprio sito web o in cartaceo presso la segreteria della scuola) per chiunque abbia necessità di segnalare situazioni a rischio di presunto o reale bullismo/cyberbullismo.
- Presenta al Collegio Docenti il documento E Safety Policy e il database di "Buone Pratiche per la Prevenzione e il Contrasto al Bullismo e Cyberbullismo" presente sulla piattaforma Elisa.
- Organizza negli spazi comuni della scuola una mostra di illustrazioni e fumetti sui temi dell'Educazione civica digitale e sugli strumenti di segnalazione.

Azioni del Direttore dei servizi generali e amministrativi

- assicura, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per garantire che l'infrastruttura tecnica della scuola sia funzionante, sicura e non aperta a uso improprio o a dannosi attacchi esterni;
- garantisce il funzionamento dei diversi canali di comunicazione della scuola (sportello, circolari, sito web, ecc.), all'interno della scuola e fra la scuola e le famiglie, per la notifica di documenti e informazioni del dirigente scolastico e dell'animatore digitale nell'ambito dell'utilizzo delle tecnologie digitali e di internet.

Azioni del ruolo del Personale scolastico (Ata, etc.)

- è consapevole dei problemi di sicurezza on-line connessi con l'uso di telefoni cellulari e dispositivi portatili;
- comprende e contribuisce a promuovere politiche di sicurezza;
- monitora l'uso di dispositivi tecnologici e attua politiche scolastiche per quanto riguarda questi dispositivi;
- segnala qualsiasi abuso anche sospetto e qualsiasi problema al Dirigente e ai responsabili della sicurezza online;
- adotta comportamenti sicuri, responsabili e professionali nell'uso della tecnologia;

Azioni dei Docenti

- si aggiornano costantemente sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di internet e sulla politica di sicurezza adottata dalla scuola, e ne rispettano il regolamento;
- garantiscono che le modalità di utilizzo corretto e sicuro delle ICT e di internet siano integrate nel curriculum di studio e nelle attività didattiche ed educative delle classi;
- garantiscono che le studentesse e gli studenti capiscano e seguano le regole per prevenire e contrastare l'utilizzo scorretto e pericoloso delle ICT e di internet;
- si accertano che le studentesse e gli studenti abbiano una buona comprensione delle opportunità di ricerca offerte dalle tecnologie digitali e dalla rete ma anche della necessità di evitare il plagio e di rispettare la normativa sui diritti d'autore;
- garantiscono che le comunicazioni digitali dei docenti con le studentesse, gli studenti e le famiglie siano svolte nel rispetto del codice di comportamento professionale, effettuate con sistemi scolastici ufficiali e secondo quanto previsto dall'Istituzione scolastica;
- assicurano la riservatezza dei dati personali trattati ai sensi della normativa vigente;
- controllano l'uso delle tecnologie digitali da parte delle studentesse e degli studenti durante le lezioni e ogni altra attività scolastica (ove consentito) e prendono adeguati provvedimenti relativi ad un utilizzo non consentito dei dispositivi digitali, appartenenti all'Istituzione scolastica o personali;
- nelle lezioni in cui è programmato l'utilizzo di Internet, guidano le studentesse e gli studenti ai siti controllati e verificati come adatti per il loro uso e controllano che nelle ricerche su Internet siano trovati e trattati solo materiali idonei;

- comunicano alle famiglie difficoltà, bisogni o disagi espressi dalle studentesse e dagli studenti (comprese le valutazioni su eventuali comportamenti inadeguati) rilevati a scuola e connessi all'utilizzo delle ICT, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo;
- segnalano qualsiasi problema o proposta di carattere tecnico-organizzativo, ovvero esigenza di carattere informativo, all'animatore digitale, ai fini della ricerca di soluzioni metodologiche e tecnologiche innovative da diffondere nella scuola e ai fini di un aggiornamento della politica adottata in materia di prevenzione e gestione dei rischi nell'uso delle ICT;
- segnalano, seguendo le indicazioni date dall'istituzione scolastica, al referente del cyberbullismo, al dirigente scolastico e alle famiglie qualsiasi abuso rilevato a scuola nei confronti degli alunni in relazione all'utilizzo delle tecnologie digitali o di internet, per l'adozione delle procedure previste dalle norme;
- Propongono, nell'ambito della trasversalità dell'insegnamento di educazione civica, dei video di approfondimento sulla sicurezza in rete e sui social, scegliendo anche tra le proposte disponibili sul sito di Generazioni connesse.

Azioni degli Studenti e delle Studentesse con la guida del docente

- essere responsabili, in relazione al proprio grado di maturità e di apprendimento, nell'utilizzo dei sistemi delle tecnologie digitali in conformità con quanto richiesto dai docenti;
- avere una buona comprensione delle potenzialità offerte dalle ICT per la ricerca di contenuti e materiali e avere consapevolezza della necessità di evitare il plagio e rispettare i diritti d'autore;
- comprendere l'importanza di adottare buone pratiche di sicurezza on-line quando si utilizzano le tecnologie digitali;
- adottare condotte rispettose degli altri anche quando si comunica in rete;
- esprimere domande o difficoltà o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o di internet ai docenti e agli adulti di riferimento.

Azioni delle Famiglie

- Sostenere la linea di condotta che la Scuola ha adottato nei confronti dell'utilizzo delle tecnologie dell'Informazione e delle Comunicazioni nella didattica;
- Seguire gli alunni nello studio a casa, adottando i suggerimenti e le condizioni d'uso delle ICT indicate dai docenti; in particolare, controllare l'utilizzo del pc e di internet;
- Concordare con i docenti linee di intervento coerenti e di carattere educativo in relazione ai problemi rilevati per un

uso non responsabile o pericoloso delle tecnologie digitali o di internet;

- Fissare delle regole per l'utilizzo del computer e tenere sotto controllo l'uso che i figli fanno di internet e dello smartphone in generale.

Azioni degli Enti educativi esterni e associazioni

- mantenere sempre un elevato profilo personale e professionale, eliminando atteggiamenti inappropriati;
- ascoltare e prendere in seria considerazione le opinioni ed i desideri dei minori, soprattutto se preoccupati o allertati per qualcosa;
- conoscere e rispettare le regole del nostro Istituto che esplicitano le modalità di utilizzo dei 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;
- 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);
- conformarsi alla politica della Scuola riguardo all'uso consapevole della Rete e delle TIC;
- promuovere comportamenti sicuri e la sicurezza online;
- assicurare la protezione degli studenti e delle studentesse durante le attività che si svolgono insieme;
- qualora si verificassero episodi che mettono in pericolo studenti e studentesse, segnalare al referente cyberbullismo e al/alla coordinatore/trice di classe.

1.3 Integrazione ePolicy nei documenti scolastici

(Il paragrafo spiega in che modo integrare il documento nel Regolamento dell'Istituto Scolastico da aggiornare con specifici riferimenti all'E-policy, così come nel RAV e all'interno del Patto di Corresponsabilità, in coerenza con le Linee Guida Miur e le indicazioni normative generali sui temi in oggetto).

La trasversalità dell'ePolicy rende necessaria una sua integrazione nell'ambito dei documenti che disciplinano il funzionamento dell'Istituto Scolastico.

Il Regolamento dell'Istituto scolastico, che rappresenta il principale punto di riferimento normativo, dovrà essere

aggiornato in modo tale da dare contezza dell'adozione dell'ePolicy, e richiamare le norme comportamentali e le procedure di utilizzo delle Tecnologie dell'Informazione e della Comunicazione in ambiente scolastico.

Anche il **Patto di Corresponsabilità educativa** tra scuola e famiglia dovrà essere integrato con gli opportuni riferimenti all'ePolicy, puntualizzando, da un lato l'impegno dell'Istituto ad organizzare eventi formativi/informativi a beneficio dei genitori, e dall'altro l'impegno di questi ultimi a partecipare in maniera proattiva a tali eventi.

Il **Piano Triennale dell'Offerta Formativa**, per la sua funzione di carta d'identità culturale e progettuale delle istituzioni scolastiche, nel quale si esplicita la progettazione curricolare, extracurricolare, educativa e organizzativa che le singole scuole adottano nell'ambito della loro autonomia, deve contenere anche le progettualità relative ad azioni media educative legate al percorso di ePolicy.

Così come il PTOF è il risultato di una consapevole concertazione fra le componenti delle istituzioni scolastiche (Dirigente Scolastico, docenti, alunni, genitori) e fra queste e il territorio, il patto di corresponsabilità rappresenta l'assunzione di responsabilità da parte di tutti coloro che svolgono un ruolo attivo nella Comunità educante.

La policy richiede l'integrazione con l'inserimento dei seguenti regolamenti:

- ALLEGATO 1: Patto di Corresponsabilità
- ALLEGATO 2: Regolamento GSuite e Dichiarazione di assunzione di responsabilità da parte degli studenti/genitori
- ALLEGATO 3: Regolamento di disciplina e sanzioni / uso del cellulare
- ALLEGATO 4: Intelligenza artificiale - Linee guida

PATTO EDUCATIVO DI CORRESPONSABILITA' STUDENTE-FAMIGLIA-SCUOLA

VISTO il D.Lgs. 16 aprile 1994, n. 297, Testo Unico delle disposizioni legislative vigenti in materia di istruzione, relative alle scuole di ogni ordine e grado;

VISTO il D.P.R. 8 marzo 1999, n. 275, Regolamento dell'autonomia scolastica;

VISTA la Legge 13 luglio 2015, n. 107, Riforma del sistema nazionale di istruzione e formazione e delega per il riordino delle disposizioni legislative vigenti;

VISTO il D.P.R. 26 giugno 1998, n. 249, Regolamento recante lo Statuto delle studentesse e degli studenti della scuola secondaria e ss.mm.ii;

VISTA la Legge 29 maggio 2017, n. 71, Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo e Linee di orientamento MIUR, ottobre 2017, per la prevenzione e il contrasto del cyber bullismo;

VISTA la Legge 20 agosto 2019, n. 92, Introduzione dell'insegnamento scolastico dell'educazione civica; VISTO il D.Lgs. 9 aprile 2008, n. 81, Testo Unico in materia di tutela della salute e della sicurezza nei luoghi di lavoro;

VISTA la Legge 6 giugno 2020, n. 41, Conversione in legge con modificazioni del decreto-legge 8 aprile 2020, n. 22, recante misure urgenti sulla regolare conclusione e l'ordinato avvio dell'anno scolastico e sullo svolgimento degli esami di Stato;

VISTI il Documento tecnico sull'ipotesi di rimodulazione delle misure contenitive nel settore scolastico, trasmesso dal CTS - Dipartimento della protezione civile in data 28 maggio 2020 e il Verbale n. 90 della seduta del CTS del 22 giugno 2020;

VISTO il documento "Quesiti del Ministero dell'Istruzione relativi all'inizio del nuovo anno scolastico", trasmesso dal CTS - Dipartimento della protezione civile in data 7 luglio 2020;

VISTA l'O.M. 23 luglio 2020, n. 69;

CONSIDERATE le esigenze del Piano Triennale dell'Offerta Formativa 2022-2025 elaborato dal Collegio dei Docenti nella seduta del 28/10/2021 sulla base dell'atto di indirizzo del Dirigente scolastico prot. 7272 del 08/10/2021, approvato dal Consiglio di Istituto nella seduta del 20/12/2021 con delibera n. 27.

CONSIDERATA l'esigenza di garantire il diritto all'apprendimento degli studenti nel rispetto del principio di equità educativa e dei bisogni educativi speciali individuali;

CONSIDERATA l'esigenza di garantire la qualità dell'offerta formativa in termini di maggior numero possibile di ore di didattica in presenza, in rapporto alle risorse a disposizione, in aule e spazi adeguatamente adattati alle esigenze scolastiche;

PRESO ATTO che la formazione e l'educazione sono processi complessi e continui che richiedono la cooperazione, oltre che dello studente, della scuola, della famiglia e dell'intera comunità scolastica; PRESO ATTO che la scuola non è soltanto il luogo in cui si realizza l'apprendimento, ma una comunità organizzata dotata di risorse umane, materiali e immateriali, che necessitano di interventi complessi di gestione, ottimizzazione, conservazione, partecipazione e rispetto dei regolamenti.

Il presente Patto sarà presentato alle famiglie in sede di assemblee di inizio anno scolastico ed agli alunni in classe dai loro docenti.

LA SCUOLA È UNA " COMUNITÀ EDUCANTE"

Questo significa che nella scuola convivono più soggetti uniti da un obiettivo comune: educare, cioè far crescere in maniera equilibrata ed armonica i giovani che fanno parte di questa comunità, svilupparne le capacità, favorirne la maturazione e la formazione.

I soggetti protagonisti della comunità sono:

- Gli studenti, centro e motivo vero dell'esistenza di una scuola;
- Le famiglie, titolari della responsabilità dell'intero progetto di crescita del giovane;
- La scuola stessa, intesa come organizzazione e come corpo docente che deve realizzare un suo progetto e una proposta educativa da condividere con gli altri soggetti.

Ogni società, ogni organizzazione, ogni gruppo sociale, per poter svilupparsi e raggiungere gli scopi per cui nasce deve avere sue regole, suoi principi, suoi obiettivi e metodi condivisi. Deve avere, in sostanza, un suo contratto sociale che, se rispettato, contribuisce a far raggiungere meglio gli obiettivi.

E' per questo motivo che anche noi, come scuola, proponiamo alle componenti fondamentali della nostra comunità un contratto, cioè un insieme di principi, di regole e di comportamenti che ciascuno di noi si impegna a rispettare per consentire a tutti di operare per il meglio.

Questo contratto va letto e volontariamente sottoscritto innanzi tutto dalla scuola, ma anche dallo studente, per la sua parte, e dalla famiglia, per gli aspetti che la riguardano.

E' un impegno che ci lega tutti.

Se tutti lo sapremo rispettare ne guadagneranno il buon funzionamento della scuola e la migliore riuscita del comune progetto educativo.

CONTRATTO DELLA SCUOLA

*LA SCUOLA SI IMPEGNA A:

1. Difendere la sicurezza dello studente attraverso un'adeguata sorveglianza in tutte le fasi della giornata scolastica; per prevenire allontanamenti dalla scuola non autorizzati dalle famiglie, la scuola effettua un attento controllo sulle richieste di giustificazione o di ingresso/uscita.
2. Controllare la frequenza alle lezioni per prevenire disagi o problemi, portando all'attenzione della famiglia eventuali comportamenti insoliti.
3. Contattare la famiglia in caso di problemi relativi a frequenza, puntualità, profitto, comportamento, in modo da poter intervenire insieme al primo insorgere di difficoltà.
4. Prevenire e controllare fenomeni di bullismo e vandalismo in collaborazione con le famiglie.
5. Prevenire e controllare fenomeni di cyberbullismo e di utilizzo scorretto delle tecnologie e dell'intelligenza artificiale (vedere E Safety Policy)
6. Organizzare eventi formativi/informativi a beneficio dei genitori sui temi del bullismo, del cyberbullismo, della sicurezza digitale e dell'intelligenza artificiale.
7. Tenere informata con regolarità la famiglia sulla situazione scolastica dello studente, allo scopo di favorire la collaborazione e di affrontare e risolvere insieme eventuali problemi.
8. Garantire la qualità dell'insegnamento attraverso l'aggiornamento dei docenti.
9. Esporre alla famiglie e agli studenti con chiarezza gli obiettivi didattici e le modalità di valutazione.
10. Creare un clima collaborativo e accogliente nel quale si possa lavorare con serenità.
11. Promuovere lo sviluppo personale dello studente attraverso l'offerta di opportunità curricolari ed extracurricolari.
12. Sostenere lo studente in difficoltà attraverso azioni di recupero e/o sostegno.
13. Favorire l'inserimento dello studente nella scuola, attraverso un Progetto accoglienza.
14. Sostenere lo studente durante tutto il percorso scolastico con attività specifiche di orientamento.
15. Porre attenzione ai problemi di carattere personale e psicologico dello studente, attraverso il Servizio ascolto e l'offerta di colloqui personali e riservati con uno specialista, compatibilmente con le risorse economiche della scuola.
16. Offrire opportunità di approfondimento, favorendo il benessere nella scuola e lo sviluppo di nuove capacità.
17. Coordinare i carichi di lavoro e programmare le verifiche, affinché lo studente sia sempre in grado di affrontare con serenità, ma in modo proficuo, il lavoro a casa.
18. Raccogliere e dare risposta ai pareri e ai suggerimenti delle famiglie.
19. Collaborare con lo studente alla costruzione delle competenze necessarie ad aiutarlo ad evidenziare e a valorizzare le proprie abilità e le proprie capacità.

IL CONTRATTO DEI GENITORI

*LA FAMIGLIA SI IMPEGNA A:

1. Collaborare con la scuola nel far rispettare allo studente i suoi impegni.
2. Sostenere lo studente nel suo lavoro a scuola e a casa.
3. Assicurare la frequenza regolare e la puntualità dello studente alle lezioni.
4. Informare la scuola in caso di problemi che possano incidere sulla situazione scolastica dello studente.
5. Cercare di partecipare ai momenti di incontro e confronto con la scuola (consigli di classe, riunioni, ecc...).
6. Giustificare sempre le assenze e i ritardi utilizzando le apposite pagine presenti sul diario scolastico.
7. Firmare per presa visione le comunicazioni e le valutazioni delle verifiche.
8. Segnalare alla scuola eventuali disservizi.
9. Segnalare situazioni critiche, fenomeni di bullismo o vandalismo, eventuali fenomeni di cyberbullismo ed eventuali usi scorretti dell'intelligenza artificiale che potrebbero verificarsi nelle classi e nella scuola.
10. Partecipare in maniera proattiva agli eventi formativi/informativi organizzati dalla scuola.
11. Prendere consapevolezza dei contenuti dell'art. 2048 del Codice Civile riguardante la responsabilità dei genitori degli eventuali danni a cose e /o persone causate dai propri figli in violazione dei doveri sanciti dal Regolamento d'Istituto.
12. Promuovere il corretto utilizzo a scuola e fuori scuola dei dispositivi elettronici. 13. Esprimere il proprio parere sulla scuola e offrire eventuali suggerimenti anche attraverso la compilazione dei questionari di soddisfazione che verranno consegnati a fine anno.

IL CONTRATTO DEGLI STUDENTI

*LA STUDENTE/LO STUDENTE SI IMPEGNA A:

1. Rispettare le persone che lavorano e che frequentano la scuola, senza discriminazione alcuna.
2. Rispettare le regole di comportamento stabilite.
3. Frequentare la scuola regolarmente e con puntualità.
4. Tenere un comportamento corretto ed adeguato all'ambiente.
5. Eseguire i lavori assegnati a casa e consegnarli con puntualità.
6. Collaborare con la scuola per mantenere l'ambiente pulito e ordinato.
7. Segnalare situazioni critiche, fenomeni di bullismo/vandalismo, di cyberbullismo e di uso scorretto dell'intelligenza artificiale, che possono verificarsi nelle classi, nella scuola e durante tutte le attività scolastiche.
8. Aiutare i compagni in difficoltà.
9. Segnalare alla scuola gli eventuali disservizi.
10. Portare a scuola tutto il materiale necessario alle lezioni.

Si rimanda a: "Diritti e doveri degli studenti" art. 12 del Regolamento di Istituto ad integrazione del Patto di Corresponsabilità

LA SCUOLA SI IMPEGNA A:

1. Collaborare con la famiglia nel far rispettare allo studente i suoi impegni.
2. Sostenere lo studente nel suo percorso volto al successo formativo.
3. Intraprendere azioni di formazione e aggiornamento del personale scolastico in tema di competenze digitali al fine di implementare e consolidare pratiche didattiche efficaci con l'uso delle nuove tecnologie, a supporto degli apprendimenti delle studentesse e degli studenti;
4. Intraprendere iniziative di alfabetizzazione digitale e di cittadinanza digitale a favore delle studentesse e degli studenti al fine di promuovere e sviluppare un uso efficace e consapevole delle nuove tecnologie nell'ambito dei percorsi personali di apprendimento;
5. Garantire la massima trasparenza negli atti amministrativi, chiarezza e tempestività nelle comunicazioni, anche attraverso l'utilizzo di strumenti informatici, garantendo il rispetto della privacy.

CARI GENITORI

Collaborate con noi ad una buona formazione, culturale ed umana, degli studenti. Vi diamo alcuni suggerimenti, derivati dalla nostra esperienza professionale, nella speranza che vogliate parlarne con i vostri figli per aiutarli a crescere.

- Se c'è qualche cosa che non funziona, sia sul piano organizzativo, sia su quello educativo e didattico, più che lamentarvi con i vostri figli o con qualche genitore di vostra conoscenza, contattate i rappresentanti di classe, oppure venite a parlare con il docente coordinatore o con l'insegnante direttamente interessato o anche, se lo ritenete necessario, ricorrete al dirigente e allo staff di presidenza. Parlando, esponendo i propri dubbi, molti problemi possono essere risolti. Soprattutto cercate di non creare un conflitto di autorità nei vostri figli.
- Cercate di essere presenti agli incontri e alle opportunità di colloquio che la scuola vi offre. La vostra partecipazione per noi è preziosa e per i vostri figli è un segno di attenzione.
- Incoraggiate i vostri figli a rispettare le regole di una convivenza civile ed armonica con gli altri e con l'ambiente.
- Tenete sotto controllo il libretto delle giustificazioni; se avete qualche dubbio che vostro figlio/a qualche volta non sia venuto a scuola senza dirvelo, venite a scuola ed accertatevi della situazione. Non coprite le marachelle, più o meno gravi, dei vostri figli, ma parlatene con loro.
- Aiutate vostro figlio a predisporre un luogo tranquillo e ben illuminato per studiare. Non mettetegli fretta, non intervenite con troppa ansia, cercate di evitare che ci sia rumore nella sua stanza e che cominci a studiare troppo tardi.
- Aiutate vostro figlio a programmare in anticipo ed ad organizzare il proprio tempo. Partecipare ad un'attività sportiva, o di altro tipo, lo aiuterà a scaricarsi e poi potrà studiare con più concentrazione.
- Parlate spesso con i vostri figli, lasciate che vi raccontino tutto ciò che è successo in classe, chiedete loro di commentare i fatti accaduti e di darvi il loro giudizio.
- Favorite, se vi è possibile, le richieste di studiare con qualche compagno/a. All'inizio perderanno un po' di tempo, ma fate loro capire che il lavoro insieme può essere più piacevole e anche proficuo.
- Ricordatevi: essere genitori responsabili è uno dei mestieri più difficili, ma può dare tante soddisfazioni.

PROCEDURA OBBLIGATORIA DI COMPOSIZIONE: avvisi e reclami

In caso di parziale o totale inosservanza dei diritti-doveri previsti o implicati nel presente patto si attua la procedura di composizione obbligatoria, ove non si configurino come violazioni sanzionabili in modo più grave. Essa comprende l'applicazione, tramite opportuna documentazione, delle sanzioni disciplinari ispirate a criteri applicativi di gradualità e proporzionalità, rafforzando la possibilità di recupero dello studente, eventualmente anche attraverso (da valutare caso per caso) attività di natura sociale e culturale.

IMPEGNI DI RECIPROCIITA':

Il genitore/tutore/affidatario, sottoscrivendo l'istanza d'iscrizione, assume l'impegno:

- a) ad osservare le disposizioni contenute nel presente documento, dei regolamenti ivi richiamati e degli obblighi di Legge
- b) a sollecitarne l'osservanza da parte dell'alunno/a.

Il Dirigente scolastico, in quanto legale rappresentante dell'istituzione scolastica e responsabile gestionale, assume impegno affinché i diritti/doveri degli studenti e dei genitori richiamati nel patto siano garantiti.

REGOLAMENTO G SUITE FOR EDUCATION

Premessa

Come già anticipato nelle Comunicazioni della Dirigenza n.256 e n. 257, seguendo le direttive del DPCM adottate il giorno 8 marzo 2020, si informa che la Scuola Secondaria di I grado "G.Floreatini" ha attivato la piattaforma "G-Suite for Education" per offrire ai propri studenti la possibilità di usufruire di nuovi e stimolanti metodi di apprendimento, coerenti con il piano nazionale Scuola Digitale ed altresì con le odierne forme di comunicazione e sviluppo delle conoscenze supportate dalla tecnologia informatica. Per queste ragioni la piattaforma è attualmente la più utilizzata nelle scuole italiane e il suo impiego è fortemente sostenuto dal MIUR.

Attraverso il nuovo account cognome.nome@smsdomodossola.it (nel dominio smsdomodossola.it di cui l'istituto è proprietario) docenti a tempo indeterminato e determinato, personale ATA e studenti potranno usufruire delle applicazioni messe a disposizione da G Suite:

1. il servizio di posta elettronica Gmail
2. lo spazio di archiviazione Drive
3. la piattaforma Classroom
4. Meet/Hangouts
5. l'editor di testo, il foglio e la presentazione Google (Google documenti)
6. il calendario condiviso e integrato con Gmail e le app per prendere note
7. sites per la realizzazione di siti didattici

8. molte altre applicazioni tra cui anche il coding

9. successive app che verranno attivate/registreranno l'accesso dall'account Google

Gli account creati devono essere utilizzati esclusivamente per tali fini. Si ricorda infatti che le credenziali di accesso sia ai dispositivi che ai siti non sono di proprietà dell'utente finale ma unicamente del provider che eroga il servizio e sono, pertanto, affidati all'utente solo per gli scopi previsti.

Le applicazioni a disposizione dell'utente, fruibili via internet, sono attivabili a discrezione dell'Istituto, che ne definisce di volta in volta regole e limiti di utilizzo, anche tramite i propri docenti nello svolgimento quotidiano delle attività didattiche ed in base alle esigenze legate all'attività svolta, indipendentemente dalle possibilità tecniche offerte dalla piattaforma di Google. I responsabili sono l'Amministratore e il titolare della licenza d'uso del servizio cioè il Dirigente Scolastico.

Il servizio è fornito gratuitamente ed è fruibile fino al termine del percorso di studio degli studenti o al termine dell'attività lavorativa del personale presso l'Istituto.

Possono richiedere la creazione di un account altre categorie di utenti, sempre in relazione alle necessità didattiche e di comunicazione; in questo caso l'accoglimento della domanda, motivatamente redatta, è a insindacabile giudizio dei responsabili.

Il presente Regolamento che disciplina l'uso dei suddetti strumenti digitali è entrato in vigore a partire dall'attuale anno scolastico 2019/2020.

Il presente Regolamento comprende altresì le norme per l'accesso e l'uso dell' Aula G@lileo" e dei laboratori, nonché dei devices in dotazione all'istituto sia nella sede centrale sia nella sede di Via Ceretti, previa assunzione di responsabilità dei genitori/studenti circa le norme che ne regolano l'uso.

REGOLAMENTO G SUITE FOR EDUCATION

ARTICOLO 1 - Consenso degli interessati

STUDENTI

Ogni studente/studentessa riceverà la password per accedere ai servizi di G Suite e avrà accesso alla piattaforma solo dopo che i loro genitori/esercenti potestà genitoriale avranno accettato le regole di utilizzo, dichiarando inoltre di essere a conoscenza della normativa vigente locale, nazionale ed europea.

DOCENTI E PERSONALE ATA

Il conferimento dei dati di cui alla presente informativa ha natura obbligatoria per quanto riguarda i dipendenti dell'Istituto ai sensi di quanto previsto dall'art.47 del D.Lgs.82/2005 "Codice dell'Amministrazione Digitale" (e successive modificazioni). Pertanto non è necessario acquisire il consenso dell'interessato ma solamente fornire la presente informativa.

ARTICOLO 2 - Durata del rapporto e cessazione del servizio

STUDENTI

L' accordo per l'uso di "G Suite" con lo Studente ha durata triennale e comunque fino a conclusione del percorso di studi e viene rinnovato automaticamente all'atto dell'iscrizione all'anno successivo. Al termine del percorso scolastico o in caso di ritiro, dopo 3 mesi, l'amministrazione procederà alla disattivazione dell'account. Sarà quindi possibile recuperare i propri dati personali entro 90 giorni dalla cessazione del servizio. Successivamente l'indirizzo verrà eliminato e con esso l'intero materiale residuale e non scaricato dall'utente.

DOCENTI E PERSONALE ATA

Per i docenti/personale ATA il servizio viene reso disponibile per tutto il periodo di permanenza presso l'Istituto e cessa con il termine del contratto, oppure in caso di trasferimento ad altro Istituto. Sarà possibile per il docente/personale recuperare i propri dati personali entro 3 mesi dalla cessazione del servizio. Successivamente l'indirizzo verrà eliminato. Nel caso di supplenze brevi, l'account sarà invece revocato dopo 30 giorni dal termine del contratto.

ARTICOLO 3 - Condizioni di utilizzo

1. L'utente è responsabile dell'utilizzo del servizio e come tale si impegna a non commettere violazioni della legislazione vigente, del regolamento di Istituto e di qualsiasi ulteriore norma stabilita dall'amministratore. Si impegna altresì a rispettare le regole che disciplinano il comportamento nel rapportarsi con altri utenti ("Netiquette") e a non ledere i diritti e la dignità delle persone.
2. Ogni account è associato ad una persona fisica ed è strettamente personale. Le credenziali di accesso non possono, per nessun motivo, essere comunicate ad altre persone.
3. L'utente è responsabile delle azioni compiute tramite il proprio account e, pertanto, esonera l'Istituto da ogni pretesa o azione che dovesse essere rivolta all'Istituto medesimo da qualunque soggetto, in conseguenza di un uso improprio.
4. Gli utenti prendono atto che è vietato servirsi o dar modo ad altri di servirsi del servizio di posta elettronica e delle applicazioni Google messe a disposizione dall'Istituto per danneggiare, violare o tentare di violare il segreto della corrispondenza e il diritto alla riservatezza.
5. Gli utenti si impegnano, inoltre, a non trasmettere o condividere informazioni che possano presentare forme o contenuti di carattere pornografico, osceno, blasfemo, diffamatorio o contrario all'ordine pubblico o alla legislazione vigente in materia civile, penale ed amministrativa.
6. Ogni singolo utente manleva l'Istituto, sostanzialmente e processualmente, sollevandolo da ogni responsabilità, danno, arrecato a se stesso o a terzi, costo o spesa, incluse le spese legali, derivanti da ogni violazione delle suddette norme.

ARTICOLO 4 - Obblighi degli utenti

OBBLIGHI DELLO STUDENTE

Lo Studente/La studentessa si impegna a:

- modificare (per tramite del genitore/esercente potestà genitoriale) immediatamente al primo ingresso la password provvisoria che gli/le sarà consegnata in modo che nessuno possa utilizzare impunemente la password altrui;
- conservare la password personale, non comunicarla e non consentirne l'uso ad altre persone (solo i genitori/esercenti potestà genitoriale) possono esserne custodi);
- assicurarsi di effettuare l'uscita dall'account e di rimuovere l'account dalla pagina web qualora utilizzi dispositivi non personali o ai quali potrebbero avere accesso altre persone;
- comunicare (per tramite del genitore/esercente potestà genitoriale) immediatamente attraverso e-mail all'amministratore l'impossibilità ad accedere al proprio account o il sospetto che altri possano accedervi;
- non consentire ad altri, a nessun titolo, l'utilizzo della piattaforma G Suite;
- non diffondere eventuali informazioni riservate di cui venisse a conoscenza, relative all'attività delle altre persone che utilizzano il servizio;
- essere responsabile di quanto viene da lui fatto nella chat e nella classe virtuale;
- non comunicare il codice di accesso alla classe a coloro che non ne fanno parte;
- accettare e rispettare le regole del comportamento all'interno della classe virtuale e le normative nazionali vigenti in materia di utilizzo di materiali in ambienti digitali, che elenchiamo nelle seguenti pagine di questo documento e che saranno anche pubblicate all'interno della classe virtuale;
- attenersi alle regole incluse nella Netiquette
- non pubblicare immagini, attività didattiche od extra-didattiche all'interno della classe virtuale senza previa autorizzazione dell'insegnante titolare della classe stessa.

Lo studente/ssa e genitori/esercenti potestà si assumono la piena responsabilità di tutti i dati da loro inoltrati, creati e gestiti attraverso la piattaforma G Suite.

OBBLIGHI DEL DOCENTE E DEL PERSONALE ATA

Il docente e il personale ATA si impegna a:

- modificare immediatamente al primo ingresso la password provvisoria che gli/le sarà consegnata in modo che nessuno possa utilizzare impunemente la password altrui;
- conservare la password personale, non comunicarla e non consentirne l'uso ad altre persone;
- assicurarsi di effettuare l'uscita dall'account e di rimuovere l'account dalla pagina web qualora utilizzi dispositivi non personali o ai quali potrebbero avere accesso altre persone;

- comunicare immediatamente attraverso e-mail all'amministratore l'impossibilità ad accedere al proprio account o il sospetto che altri possano accedervi;
- non utilizzare la stessa password per G Suite e Registro Elettronico,
- non consentire ad altri, a nessun titolo, l'utilizzo della piattaforma G Suite;
- non diffondere eventuali informazioni riservate di cui venisse a conoscenza, relative all'attività delle altre persone che utilizzano il servizio;
- essere responsabile di ogni proprio intervento nell'utilizzo delle applicazioni disponibili sulla piattaforma G Suite;
- attenersi alle regole incluse nella Netiquette.

ARTICOLO 5 - Violazioni del Regolamento – Sanzioni disciplinari

A fronte di violazioni del presente Regolamento da parte dello studente/ssa, l'insegnante titolare della classe virtuale e/o l'Amministratore comunicherà in modo orale e/o scritto quanto accaduto alla famiglia.

L'accaduto sarà anche comunicato al Consiglio di Classe che ne potrà tener conto nel determinare il giudizio del comportamento e/o adottare altri provvedimenti (*) in conformità con il Regolamento d'Istituto, il Patto di Corresponsabilità, il Regolamento Disciplinare e il documento programmatico E- Safety dell'Istituto.

Preso atto della violazione, e del parere espresso dall'insegnante titolare della classe virtuale e/o del Consiglio di Classe, il Dirigente Scolastico potrà sospendere l'account dell'utente e impedirne l'accesso immediato alla piattaforma per un dato periodo o revocarlo in modo definitivo senza alcun preavviso e senza alcun addebito a suo carico e fatta salva ogni altra azione di rivalsa nei confronti dei responsabili di dette violazioni.

Sanzioni disciplinari: Fatte salve le conseguenze di natura penale, civile e amministrativa, possono essere applicate le seguenti sanzioni:

1. il richiamo verbale;
2. il richiamo scritto- nota sul registro;
3. sospensione dalle attività scolastiche in presenza /distanza
4. il risarcimento del danno provocato.

La violazione degli obblighi da parte del personale docente e ATA verrà sanzionato secondo le prescrizioni di legge e sotto il profilo disciplinare.

Le azioni sono comminate dal Dirigente Scolastico.

Chiunque e con qualsiasi mezzo può segnalare al Dirigente Scolastico, o ai Responsabili della rete, qualsiasi violazione di quanto previsto nel presente regolamento. Le segnalazioni anonime non verranno prese in considerazione.

ARTICOLO 6 - Limiti di Responsabilità

L'Istituto non si ritiene responsabile di eventuali malfunzionamenti del servizio e si impegna affinché la piattaforma G Suite funzioni nel migliore dei modi.

L'istituto si avvale del servizio offerto dal fornitore Google Inc. con sede in 1600 Amphitheatre Parkway Mountain View, CA 94043, denominato "Google Suite for Education". Pertanto l'istituto non ha alcun potere per quanto concerne le misure necessarie a minimizzare il rischio di perdita d'informazioni e a garantire la riservatezza dei dati, ma si affida alle garanzie di sicurezza fornite da Google nel contratto di licenza d'uso sottoscritto dalla scuola. Le politiche di gestione dei dati operate dal fornitore e le garanzie di sicurezza sono descritte nel sito ufficiale dello stesso <https://support.google.com/a/answer/60762?hl=it> e <https://support.google.com/googlecloud/answer/6057301?hl=it>.

- L'utente solleva l'istituto da ogni responsabilità ed obbligazione in relazione alla cancellazione, al danneggiamento, o alla mancata conservazione dei contenuti nonché al mancato invio/ricezione di messaggi di posta (email).
- Non sono previste attività di backup e di ripristino da parte dell'istituto dato che i server sono gestiti dal fornitore. L'utente provvederà per proprio conto alla realizzazione delle copie di sicurezza che ritenesse necessarie.
- L'istituto si riserva la possibilità di sospendere temporaneamente o disattivare definitivamente il servizio.

ARTICOLO 7 - Riservatezza dei dati personali

L'istituto si impegna ad utilizzare i dati relativi all'utente nel rispetto del D.Lgs.196/2003 e successive modifiche e integrazioni e del D.Lgs.101/2018 (Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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), Provvedimento del 26 marzo 2020- Didattica a distanza : prime indicazioni (9300784) ai soli fini della creazione e mantenimento dell'account.

Il servizio è erogato dal fornitore che applica la propria politica alla gestione della privacy; l'utente può conoscere in dettaglio tale politica visitando il sito web del fornitore. <https://support.google.com/a/answer/60762?hl=it>
<https://support.google.com/googlecloud/answer/6057301?hl=it>

ARTICOLO 8 - Netiquette (Network Etiquette)

Come esistono buone regole di convivenza civile alla base dei rapporti tra le persone esiste anche un galateo della Rete (Netiquette) che ogni utente deve seguire affinché il servizio possa funzionare nel miglior modo possibile. L'utente è tenuto a:

- non inviare mai lettere o comunicazioni a catena (es. catena di S. Antonio o altri sistemi di carattere "piramidale") che causano un inutile aumento del traffico in rete;
- non utilizzare la piattaforma in modo da danneggiare, molestare o insultare altre persone; a questo proposito è bene ricordare di non scrivere tutto in maiuscolo perché equivale ad urlare un messaggio;
- non creare e non trasmettere immagini, dati o materiali offensivi, osceni o indecenti;
- non creare e non trasmettere materiale offensivo per altre persone o enti;
- non creare e non trasmettere materiale commerciale o pubblicitario se non espressamente richiesto;
- quando si condividono documenti non interferire, danneggiare o distruggere il lavoro degli altri utenti;

- non curiosare nei file e non violare la riservatezza degli altri utenti;
- usare il computer e la piattaforma Google Suite in modo da mostrare considerazione e rispetto per tutti gli altri utenti.

A questa prima serie di regole si aggiungono quelle previste nel documento programmatico E-Safety di Istituto di cui questo Regolamento costituisce parte integrante. Ogni utente ricerca informazioni, trova materiale, recupera documenti, scarica foto, video e musica, partecipa a chat sui social. In altre parole agisce in un contesto diverso da quello della vita reale. Quindi è necessario ricordare che:

- bisogna inserire nei lavori solo immagini di cui si è proprietari e/o non coperte da copyright e brani musicali non sottoposti a diritti d'autore;
- non bisogna copiare e incollare senza citare la fonte legittima perché ci si approprierebbe di scritti che sono il risultato di tempo e fatica di altri;
- ci si deve basare su siti affidabili per non incorrere nelle fake news;
- non ci si deve nascondere dietro pseudonimi e avatar (in questo senso la piattaforma G Suite educa l'utente perché l'account mostra chiaramente nome e cognome).

NORME PER L'UTILIZZO DI AULE MULTIMEDIALI E DISPOSITIVI BASATI SU ANDROID E CHROME

Approvato dal Consiglio di Istituto

Premessa

L'attrezzatura informatica costituisce patrimonio comune. Il rispetto e la tutela delle attrezzature sono condizioni indispensabili per l'utilizzo e l'efficienza dei materiali stessi.

Atti di vandalismo o di sabotaggio verranno perseguiti nelle forme previste, compreso il risarcimento degli eventuali danni arrecati.

L'accesso ai Laboratori è subordinato all'accettazione del presente Regolamento.

Si ricorda che qualsiasi cosa si faccia su un computer, resta traccia sul disco rigido, analizzabile da personale tecnico competente. Qualsiasi abuso fatto sarà controllato e saranno assunti i provvedimenti più idonei nei confronti di coloro che se ne saranno resi responsabili.

Disposizioni generali

Art.1

E' severamente vietato l'accesso agli studenti ed alle studentesse nella sala docenti ed in particolare è vietato loro l'uso dei pc dedicati ai docenti (vista la delicatezza dei dati presenti su quei PC si prega di rispettare rigorosamente questa regola).

Art.2

Tenere i computer dell'Aula Docenti puliti, non lasciare alcun documento sul desktop ma salvarlo nella cartella Docenti. Si richiede un uso responsabile delle stampanti.

Art.3

Uso aula STEM

1. prenotare l'ora nel modulo apposito posto sulla porta dell'aula;
2. in caso di anomalie di funzionamento segnalare il problema all'animatore digitale (Prof. Cogliandro Andrea) attraverso il modello che si trova sul sito nell'area riservata "modulistica da inviare all'Animatore Digitale" all'indirizzo cogliandro.andrea@smsdomodossola.it

Art.4

In tutte le Aule con LIM:

- non staccare mai i cavi di collegamento del portatile alla LIM per usare il pc da solo;
- non lasciare mai l'impianto acceso dopo l'uso;
- consentire agli studenti/studentesse l'uso della LIM solo ed esclusivamente per motivi didattici.

Art.5

L'insegnante che usufruisce dei Laboratori si impegna a vigilare sulle attrezzature.

Art.6

L'aula va lasciata in ordine come trovata con tavoli e sedie.

I notebook sono sistemati nell'armadietto in ordine di numerazione e così vanno riposti dopo l'utilizzo.

Se è necessario salvare materiali prodotti, il percorso è il seguente:

- DOCUMENTI,
- CLASSI,
- creare la cartella con il nome della propria classe (Esempio: 3E.2019) creare la cartella col nome dell'alunno nella quale verrà salvato ogni documento.

Tutti i file salvati sul desktop verranno cancellati.

Art.7

Ogni studente potrà utilizzare i laboratori esclusivamente per svolgere lavori e progetti scolastici o ad attività didattica, mai da solo ma con un insegnante di riferimento che si assume la responsabilità del laboratorio.

Art.8

Il laboratorio non deve mai essere lasciato aperto e incustodito quando nessuno lo utilizza.

Art.9

Non è ammesso l'uso privato delle postazioni e dei dispositivi.

Art.10

È assolutamente vietato portare e/o consumare cibi e bevande nel laboratorio.

Art.11

Prima di uscire dal Laboratorio occorre accertarsi che le sedie siano al loro posto, che l'aula sia pulita, che tutte le apparecchiature elettriche siano spente (salvo diverse disposizioni del tecnico) e che la porta venga chiusa a chiave.

Art.12

È assolutamente vietata qualsiasi manomissione o cambiamento dell'hardware o del software delle macchine ed è vietato modificare aspetto e configurazione del desktop.

Art.13

E' opportuno che negli ultimi 5 minuti prima del suono della campanella gli alunni e i docenti ripristino le condizioni iniziali del laboratorio. In tutti i casi, al cambio dell'ora, la classe che subentra attenderà disciplinatamente l'uscita dei compagni fuori dal laboratorio.

Art.14

È severamente proibito alle/agli alunne/i e ai docenti introdurre autonomamente programmi di qualunque natura o fare uso di giochi software nel laboratorio.

Disposizioni sull'uso di Internet

Art.15

L'accesso a Internet è consentito, nei limiti concessi da filtri e protezioni installati come da disposizione della dirigenza, solo agli insegnanti e alle classi da questi accompagnate e sotto la responsabilità del docente stesso.

Art.16

L'uso che viene fatto di Internet deve essere esclusivamente di comprovata valenza didattica.

Art.17

È vietato alterare le impostazioni del software di navigazione, scaricare programmi da Internet per utilizzarli sui computer dell'aula.

Art.18

È vietata la navigazione su siti internet potenzialmente pericolosi e/o illegali. L'uso di Internet e della posta elettronica va fatto sotto lo stretto controllo dei docenti, che non devono assolutamente lasciare incustoditi gli alunni davanti al computer con cui effettuano il collegamento.

Norma finale

Art.19

L'utilizzo di tutte le dotazioni informatiche da parte di chiunque, comporta l'integrale applicazione del presente Regolamento.

NORME BYOD STUDENTI (*) cfr. documento E- Safety di Istituto

DICHIARAZIONE DI ASSUNZIONE DI RESPONSABILITÀ DA PARTE DEGLI STUDENTI/GENITORI

Gentili genitori, l'Istituto amministra la "Google Suite For Education" e la mette a disposizione di studenti e docenti per ampliare l'offerta didattica, implementare le competenze digitali e offrire la possibilità di usufruire di nuovi e stimolanti

metodi di apprendimento, coerenti con il piano nazionale Scuola Digitale ed altresì con le odierne forme di comunicazione e sviluppo delle conoscenze supportate dalla tecnologia informatica. Per queste ragioni la piattaforma è attualmente la più utilizzata nelle scuole italiane e il suo impiego è fortemente sostenuto dal MIUR.

Ogni docente e ogni studente/studentessa potrà avere a disposizione un account cognome.nome@smsdomodossola.it

attraverso il quale usare le varie applicazioni Google secondo precise indicazioni dei docenti. Si tratta di un servizio SaaS (Software as a Service), in questo caso sviluppato e gestito da Google. Un vero e proprio sistema aziendale e quindi professionale che viene utilizzato sempre più nel mondo del lavoro e che richiama ciascun utente al rispetto di norme precise che sono le stesse che disciplinano l'uso delle piattaforme on line. Norme contenute nei seguenti decreti:

- Decreto Legislativo 10 Agosto 2018, n.101
- Il Regolamento Ue 2016/679
- Decreto Legislativo 30 giugno 2003, n. 196
- Decreto del Presidente della Repubblica 28 dicembre 2000 n. 445 e successive modifiche e integrazioni
- DECRETO 14 novembre 2007, n.239
- DPCM 8 marzo 2020

Affinché il servizio possa funzionare al meglio l'istituto stabilisce le seguenti regole.

- Dichiarazione di assunzione di responsabilità

Lo studente riceve la password per accedere ai servizi di Google Apps quando lui e un suo genitore/esercente potestà genitoriale sottoscrivono e consegnano agli insegnanti le presenti regole di utilizzo, dichiarando così di averle accettate e di essere a conoscenza della normativa nazionale e europea vigente e delle norme d'Istituto. È solo in tal modo che lo studente potrà accedere alla piattaforma di Apps di Google.

- Durata del rapporto

Il rapporto con lo studente per l'uso di "Google Suite for Education" ha durata annuale e viene rinnovato automaticamente all'atto delle successive iscrizioni.

● Obblighi dello studente

Lo studente si impegna a:

- conservare la password personale e a non consentirne l'uso ad altre persone;
- comunicare immediatamente (per tramite del genitore/esercente potestà genitoriale), attraverso mail, agli amministratori l'eventuale impossibilità ad accedere al proprio account o il sospetto che altri possano accedervi;
- non consentire ad altri, a nessun titolo, l'utilizzo della piattaforma G-Suite;

→ non diffondere eventuali informazioni riservate di cui venisse a conoscenza, relative all'attività delle altre persone che utilizzano il servizio;

→ osservare il presente regolamento, pena l'adozione di provvedimenti esplicitati dopo le regole di Netiquette.

Lo studente e la sua famiglia si assumono la piena responsabilità di tutti i dati da lui creati, gestiti e condivisi attraverso la piattaforma G Suite.

- Limiti di Responsabilità

L'Istituto non si ritiene responsabile di eventuali danni arrecati allo studente a causa di guasti e/o malfunzionamenti del servizio e si impegna affinché la piattaforma G Suite funzioni nel migliore dei modi.

L'Istituto chiede ai genitori di sottoscrivere la dichiarazione A riportata in calce al presente documento e di riconsegnarla al docente referente.

- Netiquette (Network Etiquette) per lo studente

Cortesia ed educazione, che regolano i rapporti comuni tra le persone, valgono anche in questo contesto:

- non inviare mai lettere o comunicazioni a catena (es. catena di S. Antonio o altri sistemi di carattere "piramidale") che causano un inutile aumento del traffico in rete;
- non utilizzare la piattaforma in modo da danneggiare, molestare o insultare altre persone; a questo proposito è bene ricordare di non scrivere tutto in maiuscolo perchè equivale ad urlare un messaggio;
- non creare e non trasmettere immagini, dati o materiali offensivi, osceni o indecenti;
- non creare e non trasmettere materiale offensivo per altre persone o enti;
- non creare e non trasmettere materiale commerciale o pubblicitario se non espressamente richiesto;
- quando condividi documenti non interferire, danneggiare o distruggere il lavoro dei tuoi docenti o dei tuoi compagni;
- non curiosare nei file e non violare la riservatezza degli altri studenti;
- usa il computer e la piattaforma G Suite in modo da mostrare considerazione e rispetto per compagni e insegnanti.

A questa prima serie di regole si aggiungono quelle previste nel documento programmatico E-Safety di Istituto di cui questo Regolamento costituisce parte integrante.

Ogni utente ricerca informazioni, trova materiale, recupera documenti, scarica foto, video e musica, partecipa a chat sui social. In altre parole agisce in un contesto diverso da quello della vita reale. Quindi è necessario ricordare che:

- bisogna inserire nei lavori solo immagini di cui si è proprietari e/o non coperte da copyright e brani musicali non sottoposti a diritti d'autore;
 - non bisogna copiare e incollare senza citare la fonte legittima perché ci si approprierebbe di scritti che sono il risultato di tempo e fatica di altri;
 - ci si deve affidare a siti affidabili per non incorrere nelle fake news
-
- non ci si deve nascondere dietro pseudonimi e avatar (in questo senso la piattaforma G Suite educa l'utente perché l'account mostra chiaramente nome e cognome).

A fronte di violazioni del presente Regolamento da parte dello studente, l'insegnante titolare della classe virtuale o l'Amministratore comunica in modo orale e/o scritto quanto accaduto alla famiglia.

L'accaduto viene anche comunicato al Consiglio di Classe che ne può tener conto nel determinare il giudizio di comportamento e/o per adottare altri provvedimenti (*) in conformità con il Regolamento d'Istituto, il Patto di Corresponsabilità, il Regolamento Disciplinare ed il documento programmatico E-Safety dell'Istituto.

Preso atto della violazione, e del parere espresso dall'insegnante titolare della classe virtuale e/o del Consiglio di Classe, il Dirigente Scolastico può sospendere l'account dell'utente e impedirne l'accesso immediato alla piattaforma per un dato periodo o revocarlo in modo definitivo senza alcun preavviso e senza alcun addebito a suo carico e fatta salva ogni altra azione di rivalsa nei confronti dei responsabili di dette violazioni.

(*) Sanzioni disciplinari: Fatte salve le conseguenze di natura penale, civile e amministrativa, possono essere applicate le seguenti sanzioni:

1. il richiamo verbale;
2. il richiamo scritto- nota sul registro;
3. sospensione dalle attività scolastiche in presenza /distanza
4. il risarcimento del danno provocato.

L'Istituto chiede allo studente di sottoscrivere la dichiarazione B riportata in calce al presente documento e di riconsegnarla al docente referente.

DICHIARAZIONE A

Il/La sottoscritt_.....

genitore/esercente potestà genitoriale di.....della classe.....

dichiara

di accettare le regole d'uso della piattaforma Google Suite e di autorizzare la scuola Secondaria di I grado "G. Floreanini" a creare una casella mail con estensione @smsdomodossola.it al proprio/a figlio/a.

Data.....

Firma del genitore

DICHIARAZIONE B

Io sottoscritt_alunn_ della classe

della scuola Secondaria di I grado "G. Floreanini" mi impegno a rispettare le regole di comportamento elencate nella Netiquette sopra descritte.

Data

Firma dell'allievo

ALLEGATO AL REGOLAMENTO DI ISTITUTO - REGOLAMENTO DI DISCIPLINA E SANZIONI -

I provvedimenti disciplinari hanno finalità educativa e tendono al rafforzamento del senso di responsabilità ed al ripristino dei rapporti corretti all'interno della comunità scolastica.

La segnalazione di mancanze che prevedono l'erogazione di sanzioni disciplinari, con ricaduta sul voto di condotta, è effettuata tramite:

- richiamo orale;
- nota sul diario personale;
- nota sul registro di classe;
- contestuale comunicazione al Dirigente Scolastico;
- convocazione dei genitori;
- sospensione dalle lezioni e/o dalle uscite e dai viaggi;
- esclusione dallo scrutinio finale.

Il Dirigente Scolastico unitamente al Consiglio di Classe decide le sanzioni sulla base di tali risultanze, entro 5 giorni dalla segnalazione del fatto.

Le sanzioni saranno comunicate:

- all' interessato;
- alla famiglia.

Le sanzioni sono sempre temporanee, proporzionate all'infrazione disciplinare e ispirate, per quanto possibile, al principio della riparazione del danno.

Il temporaneo allontanamento dello studente dalla classe può essere disposto solo in casi gravi o reiterate infrazioni disciplinari, per periodi non superiori ai quindici giorni.

USO DEL CELLULARE

È vietato agli studenti, durante l'orario scolastico, l'uso dei cellulari, come l'uso di ogni altro strumento o comportamento estranei all'attività didattica, così come opportunamente segnalato dal Ministero della Pubblica Istruzione nella nota del 15 marzo 2007. Il divieto deriva dai doveri sanciti dallo Statuto degli studenti (D.P.R. n° 249/1998). Un uso improprio dei video cellulari, inoltre, può configurare una violazione della privacy di terze persone (Decreto Legislativo n°196/03).

È permesso l'uso del telefono fisso della scuola per gravi e urgenti motivi. È vietato l'uso del telefono cellulare o dispositivi simili per comunicare con l'esterno o per diffondere immagini non autorizzate con dati personali altrui: il non rispetto della presente norma non costituisce solo una grave mancanza sul piano disciplinare, ma si configura come un trattamento illecito di dati personali passibile di denuncia alle autorità competenti; gli alunni sono tenuti a spegnere il proprio telefono cellulare prima dell'ingresso in scuola e a mantenerlo spento in cartella; in caso di inadempienza verranno avvisate le famiglie.

Gli alunni che manchino ai doveri scolastici e contravvengano alle norme disciplinari o offendano il decoro e la morale, incorrono in sanzioni disciplinari applicate dagli organi competenti secondo gli indicatori relativi alla tipologia della mancanza disciplinare e alla frequenza della stessa:

Mancanza disciplinare:

- Lo studente ha il cellulare e/o il dispositivo in mano o sul banco
- Utilizzo del cellulare durante l'attività didattica in tutti i locali o spazi scolastici o di pertinenza
- Uso del cellulare e/o dispositivo, improprio e /o dannoso per l'immagine e il prestigio dell'Istituzione Scolastica, degli operatori scolastici, degli alunni.

Il DS e/o il CdC ha la facoltà di sostituire le sanzioni disciplinari con altri provvedimenti comprendenti:

- collaborazione ai servizi interni della scuola;
- attività a scopo sociale che possa costituire un ammonimento, come ad esempio ricerche o approfondimenti coerenti con l'infrazione commessa.

ORGANO DI GARANZIA

Contro le sanzioni disciplinari che prevedono la sospensione dalle lezioni è ammesso ricorso, da parte della famiglia dello studente all'Organo di garanzia interno all'Istituto composto da: due docenti dell'Istituto, due genitori designati dal Consiglio di Istituto, il Dirigente Scolastico. L'Organo di Garanzia rimane in carica un triennio scolastico, (ameno di surroga o rinuncia), è presieduto da un componente eletto a maggioranza nella prima seduta del Consiglio.

Il Dirigente Scolastico convoca l'Organo di Garanzia che decide in via definitiva entro 30 giorni dalla presentazione del ricorso.

Delle decisioni emesse dall'Organo di Garanzia è tenuto apposito verbale sottoscritto dal Presidente e dal Verbalizzante e conservato in Presidenza.

Contro la sanzione disciplinare decisa dal Consiglio di Classe è ammesso ricorso al Dirigente dell'Ufficio Scolastico Territoriale del VC.O. ai sensi dell'art. 328 comma 4 del T.U. 297/94.

INTELLIGENZA ARTIFICIALE

Linee guida

Il Parlamento europeo ha approvato il Regolamento sull'Intelligenza Artificiale (AI Act), che stabilisce le regole per l'utilizzo dell'IA in vari settori, inclusa la scuola. La legge sull'IA è entrata in vigore il 1 ° agosto 2024 e sarà pienamente applicabile il 2 agosto 2026, con alcune eccezioni: divieti e obblighi di alfabetizzazione in materia di IA entrati in vigore a decorrere dal 2 febbraio 2025.

Sistemi di IA vietati e ad alto rischio

Il Regolamento vieta l'utilizzo di sistemi di IA che riconoscono le emozioni degli studenti e del personale scolastico. Sono inoltre considerati ad alto rischio e soggetti a severe restrizioni i sistemi di IA utilizzati per:

- Valutare gli studenti
- Selezionare gli studenti
- Assegnare il personale alle scuole
- Monitorare gli studenti durante le prove

Per questi sistemi, i fornitori dovranno fornire istruzioni per l'uso esaustive e la loro progettazione deve prevedere la supervisione umana.

Sistemi di IA con finalità generali

I sistemi di IA con finalità generali, come ChatGPT, possono essere utilizzati a scuola, ma è necessario che sia chiaro e facilmente rilevabile quando un contenuto è un prodotto sintetico dell'IA. Questo renderà più facile stanare gli studenti che copiano facendo fare all'IA compiti e prove di esame.

La scuola deve prepararsi all'entrata in vigore del Regolamento e provvederà a:

- Valutare i sistemi di IA attualmente in uso
- Verificare se questi sistemi sono conformi al Regolamento
- Fornire formazione al personale sull'utilizzo responsabile dell'IA
- Adeguare l'organizzazione degli uffici per la supervisione dei sistemi di IA

1.4 Condivisione e comunicazione dell'ePolicy

Il paragrafo dettaglia i seguenti aspetti:

1. il curriculum sulle competenze digitali per la comunità educante (il DigComp2.2);
2. Informazione della comunità educante (in particolare le famiglie) sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali con relative informative;
3. Come comunicare e condividere l'epolicy con gli attori pubblici e privati (enti, aziende, associazioni, etc) che realizzano iniziative nelle scuole sui temi dell'educazione civica digitale con relative informative).

1. Informazione della comunità educante (in particolare le famiglie) sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali con relative informative;

L'efficacia dell'ePolicy è direttamente proporzionale a livello di conoscenza e diffusione all'interno della comunità scolastica ivi comprese le famiglie. Il documento rappresenta il canale interno privilegiato per informare, responsabilizzare e collaborare sui temi della rete e delle tecnologie a scuola con l'intera comunità scolastica.

In tal senso, il documento è accompagnato da versioni, allegate e sintetiche, all'interno delle quali sono individuati gli elementi principali del documento; una versione è diretta agli studenti ed una è diretta alle famiglie con un linguaggio e una presentazione dei contenuti adeguata, flessibile e chiara. La versione sintetica rivolta agli studenti è inserita all'interno delle attività didattiche dell'educazione alla cittadinanza mentre la versione per le famiglie è consegnata nel corso dei colloqui scuola-famiglia.

Il documento è altresì pubblicato sul sito della scuola ed inserito nel Patto di corresponsabilità.

2. Come comunicare e condividere l'ePolicy con gli attori pubblici e privati (enti, aziende, associazioni, etc) che realizzano iniziative nelle scuole sui temi dell'educazione civica digitale con relative informative).

La presenza dell'ePolicy nell'Istituto scolastico è garanzia, per il territorio, della presenza di un presidio informato, sensibile e attento sulla rete e le tecnologie in relazione con i più giovani.

In questo senso l'Istituto può rappresentare per le Istituzioni del territorio, le aziende, e le realtà del Terzo Settore un luogo di confronto privilegiato e di sperimentazione per tutti coloro che intendono costruire progetti di cittadinanza digitale rivolte ai più giovani.

A tal fine l'adozione dell'ePolicy è comunicata all'USR di riferimento e al Municipio (servizi istruzione e servizi sociali) attraverso gli allegati sintetici progettati che indicano gli elementi del documento e le prospettive per la comunità.

Condividere e comunicare la politica di e-safety agli studenti e alle studentesse

- Tutti gli studenti e tutte le studentesse saranno informati che la rete, l'uso di Internet e di ogni dispositivo digitale

sono controllati dai docenti e utilizzati solo con la loro autorizzazione.

- L'istruzione degli studenti e delle studentesse riguardo all'uso responsabile e sicuro di internet precederà l'accesso alla rete.
- Sarà data particolare attenzione agli aspetti per i quali gli studenti e le studentesse risultano più esposti o rispetto ai quali risultano più vulnerabili.
- La scuola promuoverà eventi e/o dibattiti informativi e formativi, in momenti diversi dell'anno, rivolti agli studenti e alle studentesse, con il coinvolgimento di esperti sui temi oggetto del Documento.
- Tra le misure di prevenzione che la scuola metterà in atto ci saranno azioni finalizzate a promuovere una cultura dell'inclusione, del rispetto dell'altro e delle differenze affinché l'utilizzo di Internet, oltre che collocarsi all'interno di un sistema di relazioni, renda tutti consapevoli in una gestione trasparente dei rapporti che si sviluppano in tale ambiente, giungendo a riconoscere e a gestire le proprie emozioni. L'attivazione dello "Sportello di ascolto", rivolto a tutti gli alunni e articolato in colloqui individuali e/o collettivi, con la finalità di migliorare il benessere personale e scolastico mediante un'attività di supporto della sfera emotiva, relazionale e comportamentale, è una risorsa importante che la scuola mette in atto con la collaborazione di un esperto esterno. All'interno dello sportello, è previsto anche uno spazio riservato ai docenti e ai genitori, al fine di individuare strategie efficaci per affrontare le problematiche degli studenti.
- Una versione sintetica dell'e policy sarà inserita all'interno delle attività didattiche dell'educazione alla cittadinanza.

Condividere e comunicare la politica di e-safety al personale

- La linea di condotta della scuola, relativa alla sicurezza nell'utilizzo delle tecnologie digitali e di internet, sarà discussa negli organi collegiali e comunicata formalmente a tutto il personale con il presente documento e altro materiale informativo, anche sul sito web.
- Per proteggere tutto il personale e gli alunni, la scuola metterà in atto una linea di condotta di utilizzo accettabile, controllato e limitato alle esigenze didattiche essenziali.
- Il personale docente sarà reso consapevole del fatto che il traffico in internet può essere monitorato e si potrà risalire al singolo utente registrato.
- Un'adeguata informazione/formazione on-line del personale docente nell'uso sicuro e responsabile di internet, sia professionalmente che personalmente, sarà fornita a tutto il personale anche attraverso il sito web della scuola.
- Il sistema di filtraggio adottato e il monitoraggio sull'utilizzo delle ICT sarà supervisionato dall'animatore digitale, che segnalerà al DSGA eventuali problemi che dovessero richiedere acquisti o interventi di tecnici.

- L'animatore digitale metterà in evidenza on-line utili strumenti che il personale potrà usare con gli alunni in classe. Questi strumenti varieranno a seconda dell'età e della capacità degli alunni.
- Tutto il personale è consapevole che una condotta non in linea con il codice di comportamento dei pubblici dipendenti e i propri doveri professionali è sanzionabile.
- La scuola promuoverà eventi e/o dibattiti informativi e formativi, in momenti diversi dell'anno, rivolti a tutto il personale, con il coinvolgimento di esperti sui temi oggetto di del Documento.

Condividere e comunicare la politica di e-safety alle famiglie

- L'attenzione dei genitori sulla sicurezza nell'uso delle tecnologie digitali e di internet sarà attirata nelle news o in altre aree del sito web della scuola.
- Sarà incoraggiato un approccio di collaborazione nel perseguimento della sicurezza nell'uso delle ICT e di internet in occasione degli incontri scuola-famiglia, assembleari, collegiali e individuali.
- Una versione dell'e Policy con un linguaggio e una presentazione dei contenuti adeguata, flessibile e chiara, sarà consegnata ai genitori/tutori nel corso dei colloqui scuola-famiglia.
- L'animatore digitale fornirà alle famiglie suggerimenti e indicazioni per l'uso sicuro delle tecnologie digitali e di internet anche a casa.
- L'animatore digitale e i docenti di classe forniranno alle famiglie indirizzi sul web relativi a risorse utili per lo studio e a siti idonei ed educativi per gli alunni, sistemi di filtraggio e attività educative per il tempo libero.
- La scuola promuoverà eventi e/o dibattiti informativi e formativi, in momenti diversi dell'anno, rivolti alle famiglie, con il coinvolgimento di esperti sui temi oggetto di del Documento.

Condividere e comunicare l'ePolicy agli attori pubblici e privati (enti, aziende, associazioni, etc) che realizzano iniziative nelle scuole sui temi dell'educazione civica digitale con relative informative.

1. Definizione degli obiettivi:

- Stabilire chiaramente gli obiettivi delle iniziative di educazione civica digitale.
- Identificare i risultati attesi e come questi contribuiranno al miglioramento delle competenze digitali degli studenti.

2. Creazione di documenti informativi:

- Redigere documenti che descrivano le policy, le linee guida e le procedure da seguire.

- Includere informazioni su come le iniziative saranno implementate e monitorate.

3. Coinvolgimento degli attori:

- Identificare gli attori pubblici e privati coinvolti (es. scuole, enti locali, aziende, organizzazioni non profit).
- Presentare l'e policy attraverso slide semplificate e discutere le modalità di collaborazione.

4. Comunicazione trasparente:

- Utilizzare diversi canali di comunicazione (email, siti web, social media) per diffondere le informazioni.
- Assicurarsi che le informazioni siano accessibili e comprensibili per tutti gli attori coinvolti.
- Comunicare l'e Policy all'USR di riferimento e al Municipio (servizi istruzione e servizi sociali) attraverso gli allegati sintetici progettati che indicano gli elementi del documento e le prospettive per la comunità.

5. Monitoraggio e valutazione:

- Stabilire un sistema di monitoraggio per valutare l'efficacia delle iniziative (scheda di riscontro da inviare ai docenti delle classi coinvolte)
- Raccogliere feedback dagli attori coinvolti e apportare miglioramenti alla policy e alle procedure

1.5 - I Piani di Azione dell'ePolicy

I piani di azione rappresentano il **programma triennale** di obiettivi che la scuola intende realizzare per promuovere la conoscenza delle regole e dei protocolli di intervento che sono stati adottati con il documento di ePolicy nella comunità scolastica.

Nei Piani di Azione sono riportati **gli impegni e le responsabilità** che la scuola si assume per promuovere sui temi dell'educazione civica digitale e dell'utilizzo sicuro e consapevole delle tecnologie e della rete:

- la rilevazione dei bisogni
- le iniziative informative e formative,
- la formazione di docenti, studenti e studentesse, e famiglie,
- il monitoraggio e la valutazione delle azioni (laddove possibile, anche all'interno del RAV);

I Piani di Azione si distinguono tra standard, comuni ad ogni scuola che ha adottato l'ePolicy, e autoprodotti ovvero definiti dalla scuola sulla base del proprio contesto territoriale e delle collaborazioni in essere con Istituzioni, associazioni e aziende.

1° ANNO DI ATTIVITA' CON L'EPOLICY

MODULO I

- Realizzare un evento di presentazione dell'ePolicy ai docenti dell'Istituto;
- Realizzare un evento di diffusione dell'ePolicy in occasione degli Open Day e/o in occasione del SID dell'Istituto dedicato alle famiglie ed a studenti/esse;
- Diffondere l'ePolicy negli ambienti scolastici, a studenti e studentesse, docenti e famiglie attraverso le versioni friendly dell'ePolicy;

MODULO II

- Effettuare una rilevazione del fabbisogno formativo dei docenti sui temi dell'educazione civica digitale;
- Effettuare una rilevazione di interessi, bisogni e comportamenti delle famiglie sull'uso positivo del digitale;
- Avviare l'introduzione del kit didattico come metodo e risorsa di lavoro in alcune classi pilota;

MODULO III

- Integrare l'ePolicy (norme, regolamenti e procedure) nei documenti dell'Istituto;
- Aggiornare la Politica d'Uso Accettabile (PUA) della scuola ed il regolamento BYOD dell'Istituto;

MODULO IV

- Definizione, a partire da quanto definito nell'ePolicy, delle procedure di segnalazione anche con linguaggio child/youth friendly perché possano essere accessibili a studenti e studentesse;
- Realizzare una reportistica delle segnalazioni ricevute e dei relativi esiti.

2° ANNO DI ATTIVITA' CON L'EPOLICY

MODULO I

- Realizzare una formazione rivolta ai docenti dell'Istituto, sulla base dei risultati della rilevazione svolta nel corso del primo anno, anche attraverso il supporto di esperti/associazioni esterne o avvalendosi del percorso disponibile sul sito di Generazioni Connesse. La formazione deve coprire almeno il 60% del corpo docente.

MODULO II

- L'istituto utilizza il kit didattico come pratica metodologica e risorse a disposizione dei docenti per i percorsi di ECD attraverso la formazione specifica sviluppata per i docenti attraverso il sito di Generazioni Connesse;
- Effettuare una rilevazione di interessi, bisogni, comportamenti, abitudini di studenti e studentesse sui temi dell'educazione civica digitale;
- Realizzare una formazione rivolta agli studenti e alle studentesse attraverso il percorso previsto sulla piattaforma di Generazioni Connesse;

- Realizzare una formazione rivolta alle famiglie attraverso il percorso previsto sulla piattaforma di Generazioni Connesse

Eventi e Azioni di Presentazione e Diffusione dell'ePolicy

1. **Collegio Docenti:** Presentazione del documento e attività interattiva con un caso studio, utilizzando il video di Gaetano di Generazioni Connesse.
2. **Codice QR:** Creazione di un codice QR per accedere alla versione friendly dell'ePolicy.
3. **Database Buone Pratiche:** Utilizzo del database sulla piattaforma Elisa per la prevenzione e il contrasto al bullismo e cyberbullismo.
4. **Contest/Concorso:** Organizzazione di un concorso per studenti per creare strumenti di diffusione dell'ePolicy.
5. **Mostra:** Allestimento di una mostra di illustrazioni e fumetti sui temi dell'educazione civica digitale.

Rilevazione del Fabbisogno Formativo dei Docenti

1. **SELFIE FOR TEACHERS:** Strumento di autoriflessione sulle competenze digitali degli insegnanti, basato sul framework DigCompEdu.
2. **Questionario SELFIE:** Questionario per comprendere il livello di utilizzo positivo del digitale nell'istituto.

Rilevazione di Interessi e Bisogni delle Famiglie

1. **MYDIGISKILLS:** Questionario di autovalutazione delle competenze digitali delle famiglie, basato sul framework europeo DIGCOMP 2.2.

Team Antibullismo

1. **Riunioni Trimestrali:** Coinvolgimento di D.S., Referente Cyberbullismo, DPO, Animatore Digitale per verificare le esigenze dell'istituto.
2. **Modulo di Segnalazione:** Disponibilità di un modulo di segnalazione sul sito web della scuola o in cartaceo o su richiesta ai coordinatori di classe e ai referenti del cyberbullismo

Azioni Formative per Studenti e Studentesse

1. **Progetti Vincitori:** Ispirazione dai progetti vincitori del contest "The Kids are All Right".
2. **Video di Approfondimento:** Utilizzo dei video delle serie "We are Fearless" e "SuperErrori" per attività didattiche.

Monitoraggio e valutazione delle azioni (anche all'interno del RAV)

Monitoraggio in step

- Il monitoraggio è svolto quotidianamente da tutti i docenti nelle loro classi e dal personale della scuola nelle zone di pertinenza dell'istituto.
- Docenti, personale scolastico e famiglie si rivolgono al referente del cyberbullismo per eventuali segnalazioni.
- Il referente avvia le procedure di colloquio con i protagonisti del fenomeno e offre indicazioni al coordinatore della classe che ne darà informazione a tutto il consiglio.
- Il referente valuta con l'esperto esterno l'opportunità di un intervento su tutta la classe al fine di una ristrutturazione del contesto relazionale.
- Il referente suggerisce al coordinatore alcune attività da svolgere che riguardano l'elaborazione delle difficoltà emerse nella classe e la prevenzione.
- Il referente convoca il team per l'emergenza quando il caso lo richiede.
- L'intervento del team di emergenza può essere richiesto da tutto il personale scolastico adulto in situazioni di pericolo.
- Il referente raccoglie le proposte di attività progettuali che giungono dall'esterno (professionisti, associazioni, forze dell'ordine) e all'interno del team valuta l'opportunità di adesione di quali e quante classi.

Valutazione delle azioni

Organi preposti:

- team per l'emergenza
- consiglio di classe
- consiglio di istituto
- collegio docenti

1.6 - Le risorse di Generazioni Connesse

Risorse di Generazioni Connesse:

- [Kit Didattico](#)
- Area formazione (per docenti, famiglie, studenti/sse con ePolicy)
- Canale [Youtube](#) (webinar, video-stimolo, serie per target differenti)
- Canale [TikTok](#)
- Canale [Instagram](#)
- Canale [Facebook](#)

"Centri per un Internet più sicuro" descrive i servizi offerti dai centri per un Internet più sicuro (SIC) per informare, consigliare e assistere minori, genitori, insegnanti e prestatori di assistenza sulle questioni digitali e sulla lotta contro l'abuso sessuale su minori online.

Servizi Offerti dai SIC

1. Centro Nazionale di Sensibilizzazione:

- Organizzato dalla rete Insafe.
- Sensibilizza sulla sicurezza online e sui rischi potenziali.
- Osserva le tendenze emergenti.
- Realizza campagne e sviluppa materiale informativo.
- Organizza eventi come il Safer Internet Day.

2. Linea di Assistenza Telefonica:

- Fornisce consigli ai genitori e ai giovani su contenuti dannosi, contatti e comportamenti online.
- Affronta problemi come il cyberbullismo, il grooming e la privacy dei dati.

3. Hotline:

- Canale anonimo per segnalare contenuti illegali, come il materiale pedopornografico.

- Organizzata tramite l'Associazione internazionale delle hotline su Internet (INHOPE).

Coinvolgimento dei Giovani

Panel Giovanili:

- Offrono una piattaforma per esprimere opinioni e conoscenze sulle tecnologie online.
- I membri fungono da ambasciatori per i pari, dando consigli su come rimanere al sicuro online.

Piattaforma betterinternetforkids.eu

- Fornisce informazioni sulle ultime tendenze e sviluppi tecnologici.
- Riunisce esperti e altri portatori di interessi in materia di sicurezza online dei minori.
- Coordina eventi come il Safer Internet Day.
- Offre risorse educative e video in tutte le lingue dell'UE.

Questi centri sono cofinanziati dalla Commissione europea nell'ambito del programma Europa digitale e sono presenti nella maggior parte degli Stati membri, cooperando a livello dell'UE per migliorare la sicurezza online dei minori.

"Una strategia europea per un internet migliore per i bambini (BIK+)" descrive la nuova strategia adottata l'11 maggio 2022 per garantire che i minori siano protetti, rispettati e responsabilizzati online. Ecco un riassunto dei punti principali:

Obiettivi della Strategia BIK+

La strategia BIK+ si basa su tre pilastri fondamentali:

1. Esperienze digitali sicure:

- Proteggere i minori da contenuti, comportamenti e rischi online dannosi e illegali.
- Creare un ambiente digitale sicuro e adeguato all'età.

2. Responsabilizzazione digitale:

- Consentire a tutti i minori, inclusi quelli in situazioni di vulnerabilità, di acquisire le competenze necessarie per compiere scelte valide ed esprimersi online in modo sicuro e responsabile.

3. Partecipazione attiva:

- Dare voce ai minori nell'ambiente digitale.
- Promuovere attività guidate dai minori per esperienze digitali sicure, innovative e creative.

Iniziative e Collaborazioni

Portale Better Internet for Kids:

- Fornisce risorse e migliori pratiche.
- Collabora con la rete di centri per un Internet più sicuro negli Stati membri.

Standard di garanzia e verifica dell'età:

- Sviluppo di metodi standard per la verifica dell'età in Europa.
- Supporto alla rapida valutazione dei contenuti illegali e nocivi.

Numero 116 111:

- Offerta di aiuto alle vittime di bullismo online.

Coinvolgimento dei Giovani

Partecipazione dei giovani:

- Organizzazione di valutazioni guidate dai bambini della strategia BIK+.
- Aumento delle attività tra pari a livello nazionale, regionale e locale.

- Consultazione dei giovani utenti da parte dell'industria.

Visione e Cooperazione

Visione:

- Fornire servizi digitali adeguati all'età in cui ogni minore in Europa sia protetto, emancipato e rispettato online.
- Garantire che nessuno sia lasciato indietro.

Cooperazione:

- Coinvolgimento dell'industria e degli Stati membri per realizzare i piani.
- Condivisione di esperienze, competenze e valori con organizzazioni e partner internazionali.

La strategia BIK+ è il braccio digitale della strategia globale dell'UE sui diritti dei minori dal 2021 e continuerà a orientare l'elaborazione delle politiche in tutti gli Stati membri dell'UE.

<https://www.youtube.com/watch?v=DVBpGpAWcw&list=PL43P0iKGmv1c6KPpUH8MIBNHjwWCxwkla>

Cap 2 - Sensibilizzazione e prevenzione

2.1 - Sensibilizzazione e prevenzione

(Il capitolo raccoglie indicazioni su azioni formative per studenti/esse, famiglie e docenti con obiettivi a breve e lungo termine e riferimenti normativi (es legge 92 2019 su ECD). I rischi online andranno in appendice come glossario, sul sito come approfondimenti, sul kit didattico come attività.

La quotidianità in rete di ciascuno dei componenti della comunità scolastica - docenti, studenti e famiglie - deve essere caratterizzata da una consapevolezza critica delle caratteristiche degli ambienti e dei servizi online affiancata alle competenze per vivere al meglio il mondo connesso.

In questa direzione l'ePolicy è un documento che sviluppa azioni e interventi con l'obiettivo di raggiungere l'intera comunità scolastica e promuovere, ciascuno secondo il proprio ruolo, una cittadinanza digitale composta dalla conoscenza dei diritti in rete, dei rischi e delle opportunità per una partecipazione attiva e responsabile nella rete.

Gli studenti e le studentesse di oggi vivono "onlife" (L. Floridi, 2014), ovvero sono perennemente connessi al mondo online. Nelle nuove tecnologie vedono un ambiente cognitivo in grado di aumentare sia la loro dimensione sociale e relazionale, sia il loro bagaglio culturale. Alla luce di questo nuovo ambiente, rinnovare la metodologia didattica a scuola è fondamentale; promuovere l'uso delle tecnologie, permette di stimolare un atteggiamento attivo nei confronti degli apprendimenti (livello operativo), di sviluppare la conoscenza delle potenzialità e dei rischi che gli/le studenti/esse possono incontrare, di coltivare il senso critico, il principio della responsabilità e la riflessione metacognitiva, di educare all'inclusione ovvero al confronto e al rispetto dell'altro. Educare ai media nella scuola, significa educare alla cittadinanza. La "cittadinanza digitale" consiste nello sviluppo della capacità di un individuo di avvalersi consapevolmente e responsabilmente dei mezzi di comunicazione virtuali (L.92, 20 agosto 2019).

Linee metodologiche da sviluppare come opportunità per una partecipazione attiva e responsabile nella rete:

- *EAS, ovvero Episodi di Apprendimento Situato.* Ogni episodio è costruito su tre periodi di tempo principali: un momento anticipatorio, cioè un compito che viene consegnato alla classe e che può essere un video da guardare o un'esperienza da fare solitamente in modalità flipped, da svolgere a casa; un momento operativo in cui la classe deve sviluppare una micro-attività individuale o di gruppo nella quale bisogna produrre un artefatto (una mappa concettuale, un breve video); un momento di ristrutturazione (debriefing) ovvero una riflessione critica sui processi attivati e che si può realizzare sia attraverso un brainstorming, sia tramite metodologie di analisi più strutturate. L'insegnante conclude con una breve lezione in cui fissa i concetti-chiave e pone ulteriori approfondimenti. Questa metodologia punta a una didattica inclusiva, in quanto lavorare insieme su cose da realizzare rende possibile l'emergere della comunicazione; facendo leva sulla diversità degli alunni, mira a un'idea di scuola democratica dove valorizzare i talenti significa garantire una forma di merito che non è basata sulla competitività ma sul riconoscimento delle differenti competenze di ogni studente nella classe.
- *Cooperative Learning o apprendimento cooperativo*
- *Flipped classroom o classe capovolta*

- *Peer to peer o educazione tra pari*
- *Project-based learning o apprendimento basato su progetti*
- *Problem-based learning o apprendimento basato su problemi*
- *Learning Creative Learning o apprendimento creativo.*

Sensibilizzazione e prevenzione dei rischi online

Il minore potrebbe:

- commettere azioni online che possano danneggiare lui/lei stesso/a o altri;
- essere una vittima di queste azioni;
- osservare altri commettere queste azioni.

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.

Sensibilizzazione degli studenti e delle studentesse

- progetto "patente di smartphone" per tutte le classi prime
- progetto #sbullizziamoci per tutte le classi seconde (peer to peer con studenti del liceo opportunamente formati)
- incontri a tema con le forze dell'ordine per le classi seconde e terze
- attività scelte dal kit didattico (ed. civica) in tutte le classi
- partecipazione al concorso proposto dalla Questura di Verbania "Pretendiamo Legalità" con particolare riferimento al tema "Cittadinanza digitale e sicurezza on-line, con analisi sulle potenzialità e i rischi della rete, la ludopatia ed i rischi della web gaming e dell'intelligenza artificiale."

- Save the Children: volontari a scuola per la Giornata Internazionale della Sicurezza in Rete - Safer Internet Day.
- Spettacoli teatrali sul lato oscuro del web a cura di associazioni esterne.

Sensibilizzazione delle famiglie

- incontri a tema con esperti (forze dell'ordine, psicologi)
- presentazione progetto di generazioni connesse
- informativa e richiesta di autorizzazione all'utilizzo dei dati personali eccedenti i trattamenti istituzionali obbligatori (es. liberatoria per la pubblicazione delle eventuali foto, immagini, testi e disegni relativi al proprio/a figlio/a);
- rafforzare la collaborazione scuola/famiglia (L. 92/2019, art. 7) attraverso le integrazioni del patto di corresponsabilità.

Sensibilizzazione dei docenti

- presentazione progetto di generazioni connesse e kit didattico
- corsi di formazione sui rischi del mondo online (es. formazione patente smartphone)

Come prevenire

Sviluppare, attraverso una metodologia didattica adeguata (EAS) e attraverso le attività di sensibilizzazione, le conoscenze e le abilità relative ai temi proposti dalla Legge 20 agosto 2019, n. 92 sull'educazione alla cittadinanza digitale:

- a) analizzare, confrontare e valutare criticamente la credibilità e l'affidabilità delle fonti di dati, informazioni e contenuti digitali;
- b) interagire attraverso varie tecnologie digitali e individuare i mezzi e le forme di comunicazione digitali appropriati per un determinato contesto;
- c) informarsi e partecipare al dibattito pubblico attraverso l'utilizzo di servizi digitali pubblici e privati; ricercare opportunità di crescita personale e di cittadinanza partecipativa attraverso adeguate tecnologie digitali;
- d) conoscere le norme comportamentali da osservare nell'ambito dell'utilizzo delle tecnologie digitali e dell'interazione in ambienti digitali, adattare le strategie di comunicazione al pubblico specifico ed essere consapevoli della diversità culturale e generazionale negli ambienti digitali;
- e) creare e gestire l'identità digitale, essere in grado di proteggere la propria reputazione, gestire e tutelare i dati che si producono attraverso diversi strumenti digitali, ambienti e servizi, rispettare i dati e le identità altrui; utilizzare e condividere informazioni personali identificabili proteggendo se stessi e gli altri;
- f) conoscere le politiche sulla tutela della riservatezza applicate dai servizi digitali relativamente all'uso dei dati personali;

g) essere in grado di evitare, usando tecnologie digitali, rischi per la salute e minacce al proprio benessere fisico e psicologico; essere in grado di proteggere se' e gli altri da eventuali pericoli in ambienti digitali; essere consapevoli di come le tecnologie digitali possono influire sul benessere psicofisico e sull'inclusione sociale, con particolare attenzione ai comportamenti riconducibili al bullismo e al cyberbullismo.

Glossario dei comportamenti devianti online (Ministero della Giustizia) - descrizioni al sito:

<https://www.giustizia.it/giustizia/it/contentview.page?contentId=ART1144085>

A

[Auction fraud](#) - Frode d'asta

[Autolesionismo](#)

B

[Baiting](#) - Aizzare cani contro belve alla catena

[Bannare](#) - Bandire

C

[Candy girl](#) - Ragazza candita

[Catfish](#) - Pesce gatto

[Choking game](#) - Gioco asfissiante

[Click-baiting](#) - Esche da click

[Clickjacking](#) - Rapimento del clic

[Cryptolocker ransomware](#) - Riscatto informatico di crittografia bloccata

[Cyberbashing](#) - Maltrattamento informatico

[Cyberlaundering](#) - Riciclaggio online di denaro sporco

[Cybersquatting](#) - Occupazione abusiva di spazi virtuali

[Cyberstalking](#) - Molestia informatica

D

[Denigration](#) - Denigrazione

[Driving selfie](#) - Autoscatto alla guida

E

[Exclusion](#) - Estromissione

[Eyeballing](#) - Guardare con estremo interesse

F

[Fake](#) - Contraffatto

[Flaming](#) - Lite furibonda

G

[Grooming](#) - Prendersi cura della propria persona

H

[Harassment](#) - Vessazione

[Happy slapping](#) - Schiaffeggiamento felice

[Hentai](#) - Perversione

[Hikikomori](#) - Stare in disparte

[Hoax](#) - Beffa

I

[Impersonation](#) - Sostituzione di persona

K

[Keylogger](#) - File in cui vengono registrate le operazioni che l'utente compie

[Knockout game](#) - Gioco del "mettere qualcuno KO"

M

[Mailbombing](#) - Bombardamento tramite posta elettronica

N

[Neknominate](#)

O

[Outing and trickery](#) - Rivelazione e inganno

P

[Pharming](#) - Raggio telematico finalizzato all'acquisizione di dati personali e coltivazione

[Phishing](#) - Raggio telematico finalizzato all'acquisizione di dati personali

[Pro Ana](#) - pro- e an(oressi)a

[Pro Mia](#) - pro- e (buli)mia

[Pup](#) - Programma potenzialmente non desiderato

R

[Rickrolling](#) - Distorsione

[Romance scam](#) - Frode romantica

S

[Scam](#) - Truffa

[Sexting](#) - Sex (sesso) e texting (inviare SMS)

[Sextortion scams](#) - Sex (sesso) ed extortion (estorsione)

[Smishing and Vishing](#) - Truffa con sms

[Sniffing](#) - Fiutare

[Spamming](#) - Inondazione (di caselle di altri utenti) con messaggi indesiderati

[Spearphishing](#) - Arpione + phishing

[Spim](#) - Acronimo di Messaging Spam

[Spoofing](#) - Farsi beffa di qualcuno

[Stripnomination](#) - Nomination dello streep tease

T

[Tabnabbing](#) - Catturare la scheda di un browser

[Thinspiration](#) - Ispirazione al dimagrimento

[Troll](#) - Secchione

[Typosquatting](#) - Occupazione abusiva di spazi virtuali tramite errore di battitura

V

[Violazione dell'account](#)

W

[Whaling](#) - Caccia alla balena

2.2 - Il Curricolo Digitale

Per realizzare questo obiettivo l'istituto utilizza le risorse messe a disposizione a livello nazionale e internazionale.

Il DigComp 2.2, framework europeo sulle competenze digitali, permette di costruire una cornice precisa in cui inquadrare i temi e le corrispondenti competenze da proporre nell'Istituto non solo per gli studenti.

Al suo interno vengono identificati alcuni temi sui quali è costruita una proposta specifica per le famiglie e gli studenti (formazione). Tale cornice trova poi sviluppo specifico, per gli studenti, nel curriculum di educazione alla Cittadinanza Digitale previsto dalla L. 92/2019. Il curriculum prende forma attorno all'ePolicy e le attività didattiche sono legate al documento ed alle scelte dell'Istituto al suo interno.

Nel curriculum va previsto in ogni classe un appuntamento didattico specifico, calibrato sull'età degli alunni, e l'utilizzo dei kit didattici per favorire da parte degli studenti una maggiore conoscenza e consapevolezza delle finalità del presente documento.

I regolamenti e le attività sviluppate sul tema della prevenzione presenti nell'ePolicy sono parte, costante ma non esclusiva, delle azioni di disseminazione e sensibilizzazione descritte ed attuate dall'Istituto.

IL CURRICOLO DELLE COMPETENZE DIGITALI PER GLI/LE STUDENTI/ESSE

Scuola secondaria di primo grado

Riferimento: DigComp 2.2 - Il quadro di riferimento per le competenze digitali dei cittadini

Area di Competenza 1. Alfabetizzazione su informazioni e dati

1.1 Navigare, ricercare e filtrare dati, informazioni e contenuti digitali

1.2 Valutare dati, informazioni e contenuti digitali

1.3 Gestire dati, informazioni e contenuti digitali

Area di Competenza 2. Comunicazione e collaborazione

- 2.1 Interagire con gli altri attraverso le tecnologie digitali
- 2.2 Condividere informazioni attraverso le tecnologie digitali
- 2.3 Impegnarsi nella cittadinanza attraverso le tecnologie digitali
- 2.4 Collaborare attraverso le tecnologie digitali
- 2.5 Netiquette
- 2.6 Gestire l'identità digitale

Area di Competenza 3. Creazione di contenuti digitali

- 3.1 Sviluppare contenuti digitali
- 3.2 Integrare e rielaborare contenuti digitali
- 3.3 Copyright e licenze
- 3.4 Programmazione

Area di Competenza 4. Sicurezza

- 4.1 Proteggere i dispositivi
- 4.2 Proteggere i dati personali e la privacy
- 4.3 Tutelare la salute e il benessere
- 4.4 Tutelare l'ambiente

COMPETENZA TECNOLOGICA

- Padroneggia le diverse potenzialità di un dispositivo e sa riconoscere funzioni simili in diverse interfacce e sistemi operativi.
- Di fronte a problemi d'uso, è in grado di elaborare soluzioni.
- Opera su vari devices digitali per esplorare, documentare, selezionare, archiviare, modificare risorse veicolate da diversi linguaggi.
- Usa la rete con la guida dell'insegnante per condividere materiali ed interagire con altri.
- Si prende cura dei dispositivi che ha a sua disposizione

COMPETENZA COGNITIVA

- Ricerca, interpreta e valuta le informazioni
- Confronta le risorse rinvenute con le conoscenze proprie pregresse
- Rielabora in modo personale e/o creativo le informazioni, usufruendo di tutte le potenzialità offerte dal web (immagini, video, filmati, ecc)

COMPETENZA ETICA

- Regola il proprio consumo mediale
- Rispetta in modo consapevole e autonomo le regole della comunicazione digitale
- E' consapevole che la tecnologia implica anche un modo di relazione e quindi una responsabilità sociale; conosce le fondamentali norme che devono essere rispettate a tutela propria ed altrui fuori e dentro la rete.
- E' consapevole di ciò che produce ed è responsabile rispetto alla visibilità, permanenza e privacy dei messaggi propri ed altrui.

OBIETTIVI DI APPRENDIMENTO

Usare dispositivi tecnologici

Classe 1: Modificare, salvare ed archiviare gli elaborati

Classe 1: Esplorare la rete senza perdere di vista l'oggetto della ricerca

Classe 1: Caricare e scaricare materiali in rete

Classe 2: Riconoscere l'attendibilità di un sito

Classe 2: Conoscere più Applicazioni per creare tipologie diverse di artefatti digitali Classe 2: Distinguere la stessa App su devices diversi

Classe 2: Riconoscere App diverse da utilizzare per il medesimo obiettivo

Classe 3: Conoscere il percorso per far comunicare tra loro dispositivi diversi

Classe 3: Operare trasferimenti di documenti tra i vari devices

Classe 3: Organizzare la funzionalità dei dispositivi che ha in carico

Analizzare le modalità di utilizzo del digitale

Classe 1: Comprendere che i mezzi digitali possano essere usati anche in modo poco rispettoso, a volte offensivo se non addirittura illegale

Classe 1: Conoscere e rispettare le regole fondamentali per un uso corretto degli strumenti digitali

Classe 1: Rispettare le regole della netiquette della navigazione online

Classe 2: Riconoscere gli strumenti mediali come risorse formative

Classe 2: Portare nel formale le competenze messe in atto nel mondo informale Classe 3: Ragionare sul tempo-valore del proprio consumo mediale

Ricerca e interpretare le informazioni

Classe 1: Ampliare le proprie conoscenze

Classe 1: Cercare con criterio nella rete i materiali necessari per produrre testi mediali personali

Classe 2: Filtrare le informazioni rispettando la consegna data

Classe 3: Riconoscere l'attendibilità della fonte

Scegliere e valutare

Classe 1: Scomporre un testo mediale nelle sue parti significative fondamentali Classe 1: Ricercare e discutere significati con compagni e insegnanti per migliorare il prodotto

Classe 2: Selezionare e scegliere gli elementi necessari di un testo mediale utili allo scopo

Classe 3: Sintetizzare i contenuti provenienti da più fonti

Creare contenuti

Classe 1: Abbinare immagini a testi

Classe 1: Usare immagini, audio e musiche libere da copyright

Classe 1: Conoscere i principi costitutivi per la creazione di una presentazione

Classe 2: Effettuare semplici riprese (video interviste, foto, ecc)

Classe 2: Scegliere il linguaggio mediale più adatto al contesto e alla consegna Classe 3: Rappresentare i dati di un'osservazione attraverso tabelle, mappe, diagrammi, disegni, testi

Comunicare, condividere e partecipare

Classe 1: Inviare mail con allegati

Classe 1: Condividere materiali tramite piattaforme

Classe 2: Presentare un lavoro digitale con una certa competenza

Classe 3: Intervenire su lavori digitali proposti da altri con pertinenza

Livelli di competenza:

Classe 1 livello 2: Compiti semplici svolti in autonomia e con guida in caso di necessità

Dominio Cognitivo: ricordo

Classe 2 livello 3: Compiti ben definiti e sistematici, problemi diretti svolti in autonomia

Dominio Cognitivo: Comprensione

Classe 3 livello 4: Compiti e problemi ben definiti e non sistematici svolti in modo indipendente e in base alle necessità

Dominio Cognitivo: Comprensione

IL CURRICOLO DELLE COMPETENZE DIGITALI PER I DOCENTI

Una delle competenze chiave che ogni docente deve sviluppare è quella di saper identificare le risorse digitali che meglio si adattano agli obiettivi di apprendimento che ha definito, ai bisogni specifici degli studenti con cui opera e al proprio stile di insegnamento. Inoltre il docente:

- deve essere in grado di gestire e organizzare una molteplicità di materiali, nonché di modificare, integrare e creare le proprie risorse digitali a supporto dell'insegnamento/apprendimento;
- deve saper gestire e utilizzare in modo responsabile le risorse. Questo implica il rispetto delle norme sui diritti d'autore che regolano l'utilizzo, la modifica e la condivisione delle risorse digitali;
- deve saper proteggere i contenuti e i dati ritenuti sensibili, come, ad esempio, le verifiche digitali e i voti degli studenti;
- deve assicurare che le risorse e le attività di apprendimento proposte siano accessibili a tutti gli studenti, inclusi quelli con bisogni speciali. Considerare aspettative, abilità, abitudini e preconetti di ogni studente rispetto al digitale e rispondere in modo appropriato, anche in funzione di eventuali vincoli contestuali, fisici o cognitivi che possano condizionare l'uso delle tecnologie digitali da parte dello studente stesso;
- deve utilizzare le tecnologie digitali per rispondere ai diversi bisogni educativi dei singoli studenti, permettendo a ciascuno di procedere al proprio ritmo e a diversi livelli, definendo percorsi e obiettivi didattici individuali;
- deve adottare le misure più adatte al fine di garantire il benessere fisico, psicologico e sociale degli studenti durante l'utilizzo delle tecnologie digitali;
- deve rendere gli studenti responsabili e autonomi nell'utilizzo delle tecnologie digitali, anche nell'ottica di aiutarli ad affrontare autonomamente gli eventuali rischi.

Il quadro di riferimento sulle competenze digitali dei docenti (DigCompEdu) si articola in sei aree che si focalizzano su aspetti differenti dell'attività professionale dei docenti:

Area 1: Coinvolgimento e valorizzazione professionale

Usare le tecnologie digitali per la comunicazione organizzativa, la collaborazione e la crescita professionale

Area 2: Risorse digitali

Individuare, condividere e creare risorse educative digitali

Area 3: Pratiche di insegnamento e apprendimento

Gestire e organizzare l'utilizzo delle tecnologie digitali nei processi di insegnamento e apprendimento

Area 4: Valutazione dell'apprendimento

Utilizzare strumenti e strategie digitali per migliorare le pratiche di valutazione

Area 5: Valorizzazione delle potenzialità degli studenti

Utilizzare le tecnologie digitali per favorire una maggiore inclusione, personalizzazione e coinvolgimento attivo degli studenti

Area 6: Favorire lo sviluppo delle competenze digitali degli studenti

Aiutare gli studenti ad utilizzare in modo creativo e responsabile le tecnologie digitali per attività riguardanti l'informazione, la comunicazione, la creazione di contenuti, il benessere personale e la risoluzione dei problemi.

IL CURRICOLO DELLE COMPETENZE DIGITALI PER LE FAMIGLIE

Area di competenza 2 (DigComp 2.2): COMUNICAZIONE E COLLABORAZIONE

2.1: interagire con gli altri attraverso le tecnologie. Interagire tramite diverse tecnologie digitali e capire quali sono gli strumenti di comunicazione più appropriati per quanto riguarda la comunicazione e la collaborazione scuola/famiglia

2.2: condividere informazioni attraverso le tecnologie digitali. Condividere dati, informazioni e contenuti digitali con la scuola attraverso tecnologie digitali appropriate

2.3: esercitare la cittadinanza attraverso le tecnologie digitali. Utilizzare in modo corretto e secondo la netiquette il servizio digitale di informazione e comunicazione scuola/famiglia

2.4: collaborare attraverso le tecnologie digitali. Utilizzare gli strumenti e le tecnologie per i processi collaborativi

2.5: netiquette. Essere al corrente delle norme comportamentali e del knowhow per l'utilizzo delle tecnologie digitali e l'interazione con gli ambienti digitali.

2.6: gestire l'identità digitale in modo corretto

2.3 - Il Kit Didattico

L'e-Policy prevede, a livello macro, un lavoro di lettura e d'intenti condivisi dall'intera comunità scolastica, a livello micro, invece, immagina che la singola classe lavori anche su tematiche direttamente collegate alla sicurezza in rete, ma complesse e di non immediata ricaduta nelle programmazioni scolastiche (etica e digitale, algoritmi, datafication). A tal fine si è progettato e predisposto del materiale che possa funzionare sia da attivatore, sia d'accompagnamento ai docenti e agli studenti nella fase più delicata ed incisiva del processo di prevenzione: la lezione in classe.

Pertanto, il progetto Generazioni Connesse, a supporto del lavoro dell'e-Policy ha previsto per i docenti e studenti di ogni segmento scolare un nuovo [Kit Didattico](#) che contiene materiali per le lezioni e per il proprio aggiornamento, a partire dalla scuola d'infanzia fino alla secondaria di secondo grado. Il Kit può essere usato nella sua interezza oppure può essere oggetto di selezione e scelta, sulla base di quanto fatto dal docente.

I riferimenti metodologici del kit didattico sono 3:

1. *Il metodo EAS: Episodi di Apprendimento Situato*
2. *Il framework: DigCom 2.2*
3. *Il modello: Classificazione Internazionale del Funzionamento, della Disabilità e della Salute ICF - CT*

Il KIT didattico è strutturato nelle 5 aree tematiche del syllabo dell'Educazione Civica digitale, che comprendono un alfabeto digitale, utile ai docenti per la progettazione delle attività in relazione al profilo e alle esigenze dei propri studenti e delle proprie studentesse.

1. **Educare ai media:**

- Didattica Digitale Integrata (utilizzo di Classroom)
- DigComp 2.2 (strumento sviluppato a livello europeo per migliorare le competenze digitali dei cittadini):
- Area delle competenze 1: Informazione e alfabetizzazione su informazione e dati.
- Area delle competenze 2: Collaborazione e comunicazione.
- Area delle competenze 3: Creazione di contenuti digitali.

- Area delle competenze 4: Sicurezza.
- Area delle competenze 5: Risolvere problemi.
- New media education (ME): attività educativa e didattica finalizzata allo sviluppo dell'informazione e della comprensione critica relativi alla natura e alle categorie dei media, alle tecniche da loro impiegate per costruire messaggi e produrre senso, ai generi e ai linguaggi specifici.
- Multiliteracies: ambienti multiculturali attuali, densi di connessioni, abitati da reti. Il termine inglese integra il livello della multimedialità (e della presenza di diversi linguaggi di comunicazione) e il livello della multiculturalità (incrocio di culture e lingue).
- Media education: comprensione critica dei media, intesi non solo come strumenti, ma come linguaggio e cultura. Educare al senso critico
- Cyberstupidity: riguarda colui che usa in modo improprio, dannoso e trasgressivo le tecnologie, o anche colui che rifiuta a priori di avvicinarsi ad esse ritenendole fonte di tutti i mali. Educare alla saggezza digitale.
- Hate speech: incitamento all'odio attraverso espressioni d'intolleranza rivolte contro delle minoranze. Educare all'empatia. al rispetto della diversità e all'inclusione.
- Comunicare nei social: sviluppare e a promuovere un comportamento sano e un utilizzo intelligente della comunicazione attraverso i social; sviluppare una cultura di consapevolezza e sostegno attraverso il confronto e il dialogo; educare i genitori attraverso l'informazione e l'approfondimento; fornire agli studenti e alle studentesse un mezzo o un luogo per segnalare eventuali problemi.

2. Internet e il cambiamento in corso

- Digital storytelling, la narrazione realizzata con il supporto di strumenti e tecnologie di natura digitale.
- Metaverso: la realtà digitale che combina aspetti dei social media, del gioco online, della realtà aumentata e di quella virtuale.
- Realtà virtuale e aumentata: la realtà virtuale (Virtual Reality, VR) trasporta in un mondo completamente digitale ed immersivo, creato interamente al computer. Si tratta di una realtà simulata che permette di esplorare ambienti tridimensionali e interagire con essi in modo realistico (es. videogiochi immersivi, simulazioni di addestramento, esperienze turistiche virtuali). La realtà aumentata (Augmented Reality, AR) mira a migliorare la percezione dell'ambiente reale sovrapponendo elementi digitali interattivi al campo visivo dell'utente. Attraverso l'uso di dispositivi elettronici come smartphone, tablet o visori dedicati, l'AR permette di combinare il mondo reale con elementi virtuali in modo fluido e intuitivo (es. applicazioni e navigatori).
- STEAM: acronimo inglese riferito all'insieme delle materie scientifiche-tecnologiche-ingegneristiche. Si tratta di un apprendimento interdisciplinare atto a promuovere le abilità nel modo in cui verranno utilizzate nella forza lavoro e

nel mondo reale.

- Conformismo digitale: insieme delle riflessioni e delle azioni che portano le persone a creare profili social con l'obiettivo di soddisfare gli altri, la platea, la massa per avere popolarità e successo. E' l'adesione acritica a ciò che offre la rete, con il rischio di farsi catturare dalla fake news e dal loro business. Educare al pensiero critico.

3. **Creatività e cultura digitale**

- Nuovi alfabeti: educare alla cittadinanza digitale per combattere le disuguaglianze, l'indifferenza, l'isolamento, l'aggressione; garantire che per tutti ci sia la possibilità di acquisire una nuova grammatica "digitale", necessaria a comprendere, partecipare ed agire, per costruire il proprio futuro e quello della comunità.
- Creative commons: tutela dei diritti di autore e condivisione di materiali didattici in rete.
- Escape room nella didattica: ambienti reali o virtuali in cui bisogna cercare elementi (enigmi, indizi e soluzioni) per trovare la chiave fondamentale per evadere o fuggire da un luogo, in contesti di mistero e avventura reale e virtuale.
- Meme: sono degli elementi multimediali con fortissimo impatto comunicativo (immagini ironiche accompagnate da un breve testo con l'obiettivo di comunicare e trasmettere qualcosa di preciso attraverso l'ironia); nella didattica può essere uno strumento per produrre contenuti.
- Storyboard: "tavola della storia", intesa come racconto, che consiste in una serie di fotogrammi o pannelli visivi che delineano gli elementi chiave di una storia, progetto o presentazione.
- Storytelling: la costruzione di storie prevede un confronto e una collaborazione di tutti gli studenti del gruppo classe e consente quindi il riconoscimento dell'altro, del suo valore e del suo ruolo all'interno del costruito narrativo e della vita reale.
- Spazio pubblico e privato: gestire la comunicazione sui social con attenzione critica, creatività e responsabilità, soprattutto pensando a quattro opportunità associate al digitale: persistenza, visibilità, possibilità di diffusione e ricercabilità (boyd, 2014). La consapevolezza e la responsabilità passano anche dall'esercizio creativo, dall'abitudine a pensare mentre si crea.
- Scrivere digitale: i vantaggi e le opportunità connesse con l'utilizzo di sistemi di AI nella produzione e revisione dei testi scritti: raccontare, comporre versi, argomentare, riassumere, revisionare utilizzando in classe applicazioni di AI.

4. **Quantificazione e Computazione**

- Capitalismo della sorveglianza: raccolta e mercificazione dei dati personali da parte delle aziende. Educare alla protezione dei dati personali.
- Chat GPT: assistenti cognitivi all'apprendimento; attraverso prompt opportunamente congegnati, l'intelligenza

artificiale permette di ottenere gli esercizi e la loro risoluzioni in tempi molto rapidi. In questo modo l'insegnante può personalizzare l'apprendimento per adeguarlo agli interessi, alle inclinazioni e alle difficoltà dei singoli studenti.

- Internet delle cose: è un neologismo che spiega l'estensione di Internet agli oggetti diversi dal computer (es. stampante in 3D). Educare al miglioramento della vita.
- Pedagogia algoritmica: educare all'intelligenza artificiale per promuovere il pensiero critico sul web sociale: riflessione su come prodotti di consumo e servizi siano resi disponibili a seguito dell'operazione di profilatura dell'utente e su come il mercato sia capace di sfruttare i nostri dati per conoscere gusti e abitudini e fornire dunque servizi più aderenti al profilo dell'utente; educare con l'intelligenza artificiale per promuovere la creatività, la valutazione, la gestione del feedback e i sistemi assistivi a disposizione delle persone con disabilità; educare l'intelligenza artificiale, ovvero orientare l'algoritmo, insegnandogli a interpretare i dati secondo uno scopo specifico. Educare al pensiero critico, alla creatività e alla valutazione.
- Data literacy: è la capacità di leggere, capire, creare e comunicare le informazioni, dunque la capacità di conferire significato ai dati, di interpretarli correttamente e di raccontare un fenomeno mediante i dati, selezionando in maniera opportuna le informazioni più rilevanti.
- Coding: disciplina che ha come base il pensiero computazionale, cioè tutti quei processi mentali che mirano alla risoluzione di problemi combinando metodi caratteristici e strumenti intellettuali. Educare alla programmazione.
- Advertgaming loot box: gli advertgaming sono videogiochi concepiti e sviluppati direttamente per comunicare messaggi pubblicitari, sviluppare la riconoscibilità del marchio e generare traffico verso i siti. Possono essere basati su semplici associazioni di idee che puntano a collegare il marchio con lo stile di vita o l'ambiente in cui il gioco è sviluppato, oppure possono rivestire una struttura più complessa, in cui l'articolo pubblicizzato viene trasformato in un tassello fondamentale dell'azione del videogame, consentendo al consumatore di provare il prodotto all'interno dei confini del gioco. Le loot box sono le casse premio, ovvero contenitori fittizi, posti in vendita nei negozi virtuali di numerosi videogiochi, acquistabili con denaro reale e/o attraverso valute virtuali prive di convertibilità all'interno dei quali è possibile rinvenire oggetti utilizzabili nel gioco stesso. Può accadere che l'esperienza di gioco sia fortemente influenzata dal contenuto delle loot box e che gli utenti siano incentivati a investire importi anche ingenti, nella speranza di trovare quel singolo oggetto. Gli algoritmi che generano le loot box agiscono secondo un programma di rinforzo variabile tipico delle slot machine, dove la scommessa è accostata all'effetto eccitante che produce. Educare alla prevenzione delle dipendenze.

5. Educazione all'informazione

- Content curation: cura dei contenuti, un processo ciclico e ricorsivo di ricerca-azione, dove i contenuti sono continuamente aggiornati, riorganizzati, reinterpretati e danno luogo a ulteriori spunti di ricerca. Educare alla ricerca-azione.
- Webquest: attività di apprendimento cooperativo in cui gli studenti lavorano in gruppo per risolvere un problema o completare un progetto, utilizzando le risorse disponibili sul Web, mettendo in pratica l'insegnamento delle competenze digitali, del pensiero critico e della collaborazione tra studenti. Educare alla cooperazione.
- Post-verità: fake news, un tipo di comunicazione che si affida a una retorica basata sulle credenze e che trova

nell'elemento emotivo l'appoggio per avere la forza di affermarsi. Educare alla capacità di interpretare.

- **Impronte digitali:** quelle che ognuno lascia in ogni momento della propria presenza sulla rete, attraverso le foto che carica nei social media, i commenti che posta, i profili che segue, i "mi piace", che rimarranno per sempre come indelebile traccia sul web. Educare a un'impronta sul web di cui andare fieri e che non sia motivo di disagio in nessun contesto o in futuro
- **Civic hacking:** si tratta di trovare soluzioni alternative e creative a problemi che interessano la collettività, modificando l'uso di alcuni strumenti ed elementi per far fronte a determinate criticità. Educare al problem solving.
- **Infosfera:** insieme dei mezzi di comunicazione e delle informazioni da essi diffuse, è il frutto della coesistenza di più software (motori di ricerca, browser, applicazioni, ecc.). Al suo interno si possono distinguere due forme di monopolio: orizzontale e verticale. Ha generato la società informazionale e vede come modalità di esperienza l'onlife. Da qui la necessità di educare alla scelta consapevole che sa distinguere tra vero e falso, tra bene e male.

Il kit didattico è composto di 40 pillole teoriche e 32 schede didattiche che affrontano le tematiche inerenti ai rischi del mondo online. Le schede didattiche sono corredate dei riferimenti per i docenti di sostegno per adattare le attività a specifiche esigenze.

Esempio:

Indicatori di competenza	ICF-CY	Descrizione	Adattamenti
Gli indicatori di competenza rappresentano l'obiettivo formativo / relazionale che può essere inserito all'interno dei piani educativi individualizzati o personalizzati.	Codice ICF	La descrizione contiene la spiegazione del codice ICF- CY ed esplica l'area target cui è destinato l'indicatore di competenza	Gli adattamenti contengono gli spunti didattici utili al docente per rendere attiva la partecipazione di tutti gli alunni. La progettazione è distinta in base a diversi livelli di complessità.
Organizzare il proprio lavoro	b1641 Organizzazione e pianificazione	Capacità di organizzare sequenze di pensiero, strumenti e comportamenti volti alla realizzazione di obiettivi e azioni	1. Con l'aiuto delle PECS già predisposto dall'insegnante, chiedere al bambino di individuare gli strumenti per svolgere il compito; 2. Insieme ad un compagno, chiedere all'alunno di posizionare sul banco i materiali necessari a svolgere l'attività.
Mantenere l'attenzione sull'attività assegnata per un tempo congruo	b160 Focalizzare l'attenzione	Capacità di dirigere l'attenzione su un determinato compito ignorando stimoli distrattori.	1. Colorare il proprio autoritratto cercando di rispettare i margini. 2. Utilizzando un timer, chiedere allo studente di concentrarsi fino allo scadere del tempo. Si può utilizzare questa strategia per preparare il materiale da utilizzare successivamente.

<https://risorse.arcipelagoeducativo.it/risorse/nuovo-kit-didattico-generazione-connesse-23-24>

Cap 3 - Gestione dell'infrastruttura e della strumentazione ICT (Information and Communication Technology) della e nella scuola

3.1 - Protezione dei dati personali e GDPR

La protezione dei dati personali delle persone fisiche costituisce un diritto fondamentale. L'art. 8, par. 1, della Carta dei diritti fondamentali dell'Unione europea e l'art. 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. Le principali normative di riferimento sono il Regolamento Generale sulla Protezione dei Dati 2016/679 noto anche come GDPR, e il Dlgs 196/2003 conosciuto come Codice Privacy.

Il settore dell'istruzione è particolarmente impattato dalla tematica privacy in considerazione del fatto che gli Istituti Scolastici sono chiamati, necessariamente, a trattare un'enorme mole di dati personali.

Con l'entrata in vigore del GDPR è stato introdotto l'obbligo per ciascun Istituto scolastico di provvedere alla designazione di un Responsabile della protezione dei dati personali (RPD o DPO).

I principali obblighi in materia di protezione dei dati personali consistono nella definizione di un "organigramma privacy", nel rilascio dell'informativa al momento della raccolta dei dati e nella tenuta di un registro dei trattamenti.

Tutela dei dati personali come diritto fondamentale

Tutte le scuole hanno l'obbligo di far conoscere agli studenti, alle famiglie, ai docenti e a tutto il personale scolastico come vengono trattati i loro dati personali.

Il linguaggio dell'informativa deve essere facilmente comprensibile anche dai minori e deve contenere, in particolare, gli elementi essenziali del trattamento, specificando che le finalità perseguite sono limitate esclusivamente al perseguimento delle funzioni istituzionali necessarie per assicurare il diritto all'istruzione e alla

formazione attraverso l'erogazione dell'attività didattica.

Articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea

"Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano."

Chi tratta i dati a scuola?

All'interno della scuola, il titolare del trattamento dei dati è il dirigente scolastico, che, in quanto legale rappresentante, prende decisioni sulle attività di trattamento da intraprendere e sulle modalità attraverso cui queste verranno svolte mediante il personale amministrativo e/o docente. Tale personale è quindi autorizzato a trattare i dati nell'ambito delle attività didattiche o amministrative.

Categorie particolari di dati relativi ad alunni

Origini razziali ed etniche

I dati che rilevano le origini razziali ed etniche possono essere trattati dalla scuola per favorire l'integrazione degli alunni stranieri. Tali informazioni possono essere in alcuni casi desumibili anche dai nominativi o dai dati anagrafici degli alunni.

Convinzioni religiose

Gli istituti scolastici possono utilizzare i dati che rivelino le convinzioni religiose al fine di garantire la libertà di culto e per la fruizione dell'insegnamento della religione cattolica o delle attività alternative a tale insegnamento.

Stato di salute

I dati relativi alla salute possono essere trattati per:

- l'adozione di specifiche misure di sostegno o strumenti di ausilio per gli alunni con disabilità, con disturbi specifici di apprendimento o con Bisogni Educativi Speciali;
- la gestione delle assenze per malattia;
- l'insegnamento domiciliare e ospedaliero a favore degli alunni affetti da gravi patologie;
- la partecipazione alle attività sportive, alle visite guidate e ai viaggi di istruzione;
- in presenza di un regime alimentare differenziato dovuto a intolleranze, allergie o specifiche patologie.

Opinioni politiche

Le opinioni politiche possono essere trattate dalla scuola esclusivamente per garantire la costituzione e il funzionamento degli organismi di rappresentanza: ad es., le consulte e le associazioni degli studenti e dei genitori.

ALUNNI CON DISABILITÀ E DISTURBI SPECIFICI DELL'APPRENDIMENTO

Le istituzioni scolastiche devono prestare particolare attenzione a non diffondere, anche per mero errore materiale, dati relativi alla salute. Non è consentito, ad es., pubblicare online una circolare contenente i nomi degli studenti con disabilità. Occorre fare attenzione anche a chi ha accesso ai dati degli allievi con disabilità o disturbi specifici dell'apprendimento (DSA), limitandone la conoscenza ai soli soggetti a ciò legittimati dalla normativa scolastica e da quella specifica di settore, come ad es. i docenti, i genitori e gli operatori sanitari che congiuntamente devono predisporre il piano educativo individualizzato.

Tutela dei dati personali: norme di riferimento

Articolo 13 del GDPR

- Dati del titolare
- Dati del DPO
- Finalità e base giuridica del trattamento

- Destinatari dei dati
- Periodo di conservazione dei dati
- Diritti degli interessati

Privacy e Scuola: consenso

Il consenso privacy non è richiesto quando il trattamento dei dati è funzionale all'attività didattica e formativa, per il perseguimento di specifiche finalità istituzionali.

Il consenso privacy è richiesto per attività non strettamente connesse a quelle didattiche (ad es. per l'erogazione di corsi di musica, lezioni di lingua straniera o attività sportive, teatrali non previste dal curriculum scolastico).

Il DPO: Data Protection Officer

- E' il responsabile per la protezione dei dati, obbligatorio in tutte le scuole
- Deve avere una conoscenza approfondita della normativa privacy
- Può essere un soggetto interno o esterno all'istituto scolastico

Il DPO: compiti

- informare e fornire consulenza all'istituto scolastico e ai suoi dipendenti in merito agli adempimenti privacy;
- sorvegliare che la scuola adempia agli obblighi normativi;
- organizzare attività formative e di aggiornamento del personale;
- fornire pareri alla scuola in materia privacy;
- fungere da punto di contatto tra la scuola e il Garante Privacy.

Violazione dei dati: procedura Data Breach

In caso di violazione dei dati:

- intervenire immediatamente per interrompere la perdita di dati aggiuntiva;
- informare immediatamente e senza ritardo il Dirigente Scolastico e il Responsabile della protezione dei dati personali;
- valutare l'entità della violazione;
- valutare la necessità di procedere alla notifica della violazione al Garante Privacy.

Il registro dei trattamenti: adempimenti

Obbligo introdotto dal GDPR. E' un documento di sintesi, in cui sono riportate tutte le informazioni sui trattamenti effettuati e sulle categorie di dati utilizzati e la predisposizione di una procedura per la violazione dei dati, cosiddetto caso Data Breach. Questa procedura consente alla scuola di reagire prontamente in caso di violazione dei dati personali, ad esempio attacco informatico.

Contenuto del registro dei trattamenti:

- dati di contatto del titolare del trattamento e del responsabile della protezione dei dati;
- finalità del trattamento dei dati;
- descrizione delle categorie di interessati e delle categorie di dati personali;
- destinatari a cui i dati personali sono stati o saranno comunicati;
- trasferimenti di dati personali verso un paese terzo;
- termini previsti per la cancellazione sulle diverse categorie di dati;
- descrizione generale delle misure di sicurezza tecniche e organizzative.

3.2 - Strumenti di comunicazione online (PUA)

La Politica d'Uso Accettabile e Responsabile della Rete (P.U.A.) è un documento che racchiude una serie di regole legate

all'utilizzo della rete a scuola e a casa da parte di studenti e di tutto il personale (compresi i professionisti esterni che lavorano in contesto scolastico), integrante il DPS (Documento programmatico sulla Sicurezza). Il documento, che funge da raccordo, si compone di punti strategici riguardanti non solo i vantaggi di internet a scuola ma anche i rischi connessi all'online, nella valutazione di quei contenuti presenti in rete e di quelle azioni negative che possono comprometterne l'uso positivo. Fra queste attività: ricercare materiale non consono allo stile educativo della scuola; produrre vere e proprie azioni illecite; giocare online con la rete scolastica; violare la privacy e i diritti d'autore, etc... Nella Politica d'Uso Accettabile e Responsabile della Rete (P.U.A.) vengono definite, dunque, le regole di utilizzo fra tutti gli attori in gioco, nel rispetto dei dati sensibili di ciascuno, in particolar modo degli alunni e delle alunne.

Utilizzo dei dispositivi informatici in dotazione all'istituto

L'utilizzo dei dispositivi informatici deve avvenire in maniera responsabile ed avendo cura sia degli apparati fisici che dell'integrità dei software in essi installati. Sulla base di tali presupposti e per motivi di sicurezza, agli utenti è vietato:

- utilizzare i dispositivi per finalità personali o comunque non correlati con attività didattiche o di studio
- collegare dispositivi esterni (memorie USB, hard disk, ecc.)
- installare e disinstallare i programmi o modificarne le impostazioni
- copiare, caricare o scaricare musica, film, programmi e qualsiasi altro materiale non legato alla didattica o vincolato da copyright o comunque in conflitto con le norme dei codici civile e penale riguardanti il diritto d'autore, la privacy, la divulgazione di materiale offensivo, pedo-pornografico etc.

Accesso al Wi-Fi

Tutti i dispositivi in dotazione all'istituto devono essere dotati di credenziali per l'accesso alla rete. Tali credenziali devono essere gestite con la massima cautela e riservatezza

Utilizzo degli strumenti di didattica digitale

L'accesso alle piattaforme didattiche dell'istituto deve essere consentito esclusivamente previa autenticazione informatica. A ciascun utente devono essere fornite credenziali univoche, che devono essere custodite con la dovuta diligenza.

Registro elettronico

L'accesso al registro elettronico viene abilitato per docenti, genitori e studenti tramite credenziali di accesso da custodire con la dovuta diligenza. Il registro elettronico deve essere utilizzato esclusivamente per le finalità istituzionali predeterminate dall'istituto (es. Caricamento e lettura voti, assenze, avvisi, ecc.)

Responsabilità

- E' fondamentale che gli utenti siano pienamente consapevoli dei rischi a cui si espongono durante l'utilizzo dei dispositivi dell'istituto.
- I docenti sono responsabili dell'utilizzo dei dispositivi informatici e hanno l'obbligo di sorvegliare e responsabilizzare

gli studenti e le studentesse rispetto ad un uso consapevole e sicuro.

- Gli utenti non devono lasciare incustoditi i dispositivi informatici e devono provvedere alla disconnessione del proprio account al termine dell'utilizzo.

3.3 - BYOD

La presente ePolicy conterrà 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 infatti 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.

BYOD: Bring Your Own Device - porta il tuo dispositivo a scuola - Corrisponde all'azione #6 del Piano Nazionale Scuola Digitale (PNSD)

Vantaggi:

- accesso immediato ai materiali didattici
- personalizzazione dell'apprendimento
- sviluppo delle competenze digitali
- collaborazione online
- ricerca e approfondimento
- feedback istantaneo

La cassetta degli attrezzi:

- *GSuite* (documenti, drive, classroom, presentazioni, gmail, calendario, fogli, meet, moduli)
- *Organizzazione*: Strumenti come Simple Note e Priority List aiutano gli studenti a prendere appunti e gestire i compiti e gli impegni extrascolastici

- *Creazione di contenuti*: App come Book Creator e Canva permettono di realizzare ebook e progetti grafici, rendendo lo studio più creativo e interattivo
- *Apprendimento interattivo*: Strumenti come MindMup e Storyboard That aiutano a creare mappe mentali e storyboard per visualizzare e comprendere meglio i concetti
- *Accesso a risorse educative*: App come Wordreference e Dizionario d'italiano completo forniscono risorse linguistiche utili per lo studio delle lingue
- *Kahoot*: Una piattaforma per creare quiz interattivi che rendono l'apprendimento divertente e coinvolgente
- *I love PDF*: Strumenti per comprimere, dividere, unire e convertire file PDF, utili per la gestione dei documenti
- *Duolingo*: Un'app per l'apprendimento delle lingue straniere, ideale per un primo approccio alle lingue
- *Google Documenti e Presentazioni*: Strumenti per creare e condividere documenti e presentazioni in modo collaborativo
- *Word Wall*: Una raccolta di materiali didattici per tutte le discipline, adatta sia alla scuola primaria che secondaria
- *Padlet*: Una piattaforma per creare bacheche virtuali dove gli studenti possono collaborare e condividere idee
- *MLOL (MediaLibraryOnLine)*: Una biblioteca digitale che offre accesso a quotidiani, riviste, e-book, musica, film e molto altro

Sfide

- *Divario digitale*: La disparità di accesso alle tecnologie digitali può creare esclusione sociale e limitare le opportunità per alcune persone. È importante promuovere l'inclusione digitale e garantire che tutti abbiano accesso alle risorse tecnologiche necessarie.
- *Privacy e sicurezza*: L'uso crescente delle app digitali comporta rischi per la privacy e la sicurezza dei dati personali. È fondamentale adottare misure di protezione e sensibilizzare gli utenti sull'importanza della sicurezza online.
- *Dipendenza tecnologica*: L'uso eccessivo delle app può portare a una dipendenza tecnologica, influenzando negativamente la salute mentale e fisica. È importante trovare un equilibrio tra l'uso della tecnologia e altre attività.
- *Superficialità delle interazioni*: Le app digitali possono ridurre la profondità delle interazioni umane, rendendole più superficiali e meno significative. È essenziale mantenere relazioni autentiche e significative anche nel mondo digitale.
- *Disuguaglianze sociali*: Le tecnologie digitali possono amplificare le disuguaglianze sociali ed economiche, creando un divario tra chi ha accesso alle risorse digitali e chi no. È necessario lavorare per ridurre queste disuguaglianze e

garantire un accesso equo alle tecnologie.

Politica

1. *Regole per l'uso delle tecnologie digitali:* Le scuole adottano regolamenti specifici per l'uso delle tecnologie informatiche e della comunicazione (ICT). Questi regolamenti includono norme comportamentali e procedure per garantire un uso sicuro e responsabile delle tecnologie digitali
2. *Formazione dei docenti:* È fondamentale che gli insegnanti siano adeguatamente formati per utilizzare le tecnologie digitali nella didattica. La formazione continua dei docenti è essenziale per sviluppare competenze digitali e per integrare efficacemente le tecnologie nei processi di insegnamento e apprendimento
3. *Infrastrutture tecnologiche:* Le scuole devono disporre di infrastrutture tecnologiche adeguate, come connessioni internet veloci, dispositivi digitali e software educativi. Queste infrastrutture sono necessarie per supportare l'uso delle tecnologie digitali in classe e per garantire che tutti gli studenti abbiano accesso alle risorse digitali

Le linee guida del Ministero dell'Istruzione e altre istituzioni educative forniscono indicazioni dettagliate su come implementare e gestire l'uso delle tecnologie digitali (<https://mim.gov.it/linee-guida-per-l-uso-positivo-delle-tecnologie-digitali>)^[2](https://www.generazioniconnesse.it/_file/documenti/linee-guida/linee-guida-scuole.pdf).



DIECI PUNTI PER L'USO DEI DISPOSITIVI MOBILI A SCUOLA **BYOD - BRING YOUR OWN DEVICE**

1. OGNI NOVITÀ COMPORTA CAMBIAMENTI.

Ogni cambiamento deve servire per migliorare l'apprendimento e il benessere delle studentesse e degli studenti e più in generale dell'intera comunità scolastica.

2. I CAMBIAMENTI NON VANNO RIFIUTATI, MA COMPRESI E UTILIZZATI PER IL RAGGIUNGIMENTO DEI PROPRI SCOPI.

Bisogna insegnare a usare bene e integrare nella didattica quotidiana i dispositivi, anche attraverso una loro regolamentazione. Proibire l'uso dei dispositivi a scuola non è la soluzione.

A questo proposito ogni scuola adotta una Politica di Uso Accettabile (PUA) delle tecnologie digitali.

3. LA SCUOLA PROMUOVE LE CONDIZIONI STRUTTURALI PER L'USO DELLE TECNOLOGIE DIGITALI.

Fornisce, per quanto possibile, i necessari servizi e l'indispensabile connettività, favorendo un uso responsabile dei dispositivi personali (BYOD).

Le tecnologie digitali sono uno dei modi per sostenere il rinnovamento della scuola.

4. LA SCUOLA ACCOGLIE E PROMUOVE LO SVILUPPO DEL DIGITALE NELLA DIDATTICA.

La presenza delle tecnologie digitali costituisce una sfida e un'opportunità per la didattica e per la cultura scolastica.

Dirigenti e insegnanti attivi in questi campi sono il motore dell'innovazione. Occorre coinvolgere l'intera comunità scolastica anche attraverso la formazione e lo sviluppo professionale.

5. I DISPOSITIVI DEVONO ESSERE UN MEZZO, NON UN FINE.

È la didattica che guida l'uso competente e responsabile dei dispositivi.

Non basta sviluppare le abilità tecniche, ma occorre sostenere lo sviluppo di una capacità critica e creativa.

6. L'USO DEI DISPOSITIVI PROMUOVE L'AUTONOMIA DELLE STUDENTESSE E DEGLI STUDENTI.

È in atto una graduale transizione verso situazioni di apprendimento che valorizzano lo spirito d'iniziativa e la responsabilità di studentesse e gli studenti. Bisogna sostenere un approccio consapevole al digitale nonché la capacità d'uso critico delle fonti di informazione, anche in vista di un apprendimento lungo tutto l'arco della vita.

7. IL DIGITALE NELLA DIDATTICA È UNA SCELTA: STA AI DOCENTI INTRODURLA E CONDURLA IN CLASSE.

L'uso dei dispositivi in aula, siano essi analogici o digitali, è promosso dai docenti, nei modi e nei tempi che ritengono più opportuni.

8. IL DIGITALE TRASFORMA GLI AMBIENTI DI APPRENDIMENTO.

Le possibilità di apprendere sono ampliate, sia per la frequentazione di ambienti digitali e condivisi, sia per l'accesso alle informazioni, e grazie alla connessione continua con la classe. Occorre regolamentare le modalità e i tempi dell'uso e del non uso, anche per imparare a riconoscere e a mantenere separate le dimensioni del privato e del pubblico.

9. RAFFORZARE LA COMUNITÀ SCOLASTICA E L'ALLEANZA EDUCATIVA CON LE FAMIGLIE.

È necessario che l'alleanza educativa tra scuola e famiglia si estenda alle questioni relative all'uso dei dispositivi personali. Le tecnologie digitali devono essere funzionali a questa collaborazione.

Lo scopo condiviso è promuovere la crescita di cittadini autonomi e responsabili.

10. EDUCARE ALLA CITTADINANZA DIGITALE È UN DOVERE PER LA SCUOLA.

Formare i futuri cittadini della società della conoscenza significa educare alla partecipazione responsabile, all'uso critico delle tecnologie, alla consapevolezza e alla costruzione delle proprie competenze in un mondo sempre più connesso.

Cap 4 - Segnalazione e gestione dei casi

4.1 - Cosa Segnalare

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. Queste, inoltre, forniscono valide indicazioni anche per i professionisti e le organizzazioni esterne che operano con la scuola.

Nelle procedure sono indicate le figure preposte all'accoglienza della segnalazione e alla presa in carico e gestione del caso, nonché le modalità di coinvolgimento del Dirigente Scolastico e del Referente per il contrasto al bullismo e al cyberbullismo. 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. La condivisione avverrà attraverso assemblee scolastiche che coinvolgono i genitori, gli studenti e le studentesse e il personale della scuola, con l'utilizzo di locandine da affiggere a scuola, attraverso news nel sito della scuola e durante i collegi docenti e attraverso tutti i canali maggiormente utili ad un'efficace comunicazione.

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

Cyberbullismo: è necessario capire se si tratta effettivamente di cyberbullismo o di altra problematica. Oltre al contesto, vanno considerate le modalità attraverso le quali il comportamento si manifesta (alla presenza di un "pubblico"? Tra coetanei? In modo ripetuto e intenzionale? C'è un danno percepito alla vittima? etc.). È necessario poi valutare l'eventuale stato di disagio vissuto dagli/le studenti/esse coinvolti/e (e quindi valutare se rivolgersi ad un servizio deputato ad offrire un supporto psicologico e/o di mediazione).

Adescamento online: se si sospetta un caso di adescamento online è opportuno, innanzitutto, fare attenzione a non cancellare eventuali prove da smartphone, tablet e computer utilizzati dalla persona 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, per quanto possibile, la rimozione del materiale on-line e il blocco della sua diffusione per mezzo dei 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.

Le azioni messe in atto dalla scuola:

- interventi mirati di prevenzione universale e selettiva sul gruppo classe da parte del referente del cyberbullismo e dell'esperto esterno incaricato per il progetto dello sportello di ascolto, in collaborazione con i docenti della classe;
- percorsi di mediazione volta alla gestione positiva del conflitto, attraverso gruppi di discussione (circle time), rappresentazioni e attività di role-play sull'argomento del bullismo e del cyber-bullismo, le strategie di problem solving;
- questionario self-report da proporre agli studenti, con la finalità di indagare sulle situazioni a rischio;
- reperibilità di una scheda di prima segnalazione del fenomeno presunto, reperibile online (sito della scuola); la scheda, una volta compilata, è da inviare al referente del cyberbullismo;
- percorsi individualizzati di sostegno alle vittime, volti a incrementare l'autostima e l'assertività e a potenziare le risorse di interazione sociale, mentre i prevaricatori sono destinatari di interventi mirati a smuovere le competenze empatiche e a favorire una loro condivisione delle norme morali. Anche in relazione alle manifestazioni socio-affettive fra pari, al linguaggio sessualizzato o "volgare", al fine di evitare prevaricazioni e imbarazzo o disagio, i docenti intervengono per favorire nei loro alunni un buon rapporto con il proprio corpo e per far percepire meglio eventuali violazioni dei limiti di prossimità o di "confidenza" ed imparare ad opporvisi, per far acquisire fiducia nelle proprie sensazioni e nel proprio intuito, determinazione nel rifiutare i contatti anche "a distanza" sgradevoli o "strani", per rendere consapevoli gli alunni del diritto al rispetto dei propri limiti e di quelli altrui, per far capire ai ragazzi che l'interazione on-line deve sottostare a delle regole di buon comportamento, né più né meno della comunicazione a viso aperto, quale quella della vita reale. Inoltre la scuola, qualora rilevi una situazione psico-socio-educativa particolarmente problematica, convoca i genitori o gli esercenti la potestà per valutare con loro a quali risorse territoriali possono rivolgersi. Consiglia altresì di servirsi dello sportello di ascolto gratuito attivo presso la scuola. Promuove e supporta la richiesta delle famiglie rivolta ai Servizi Sociali dell'Ente Locale per la fruizione di servizi socio-educativi comunali e alla ASL per quanto riguarda la competenza psicologica e psicoterapeutica (Pediatria, Neuropsichiatria infantile, Consultorio Familiare).

Come prevenire

- Strutturare regole condivise e stipulare con gli studenti e le studentesse una sorta di "patto" d'aula.

- Dedicare ai temi relativi ai rischi online momenti di riflessione per sviluppare la consapevolezza degli studenti e delle studentesse
- Integrare la tecnologia nella didattica, mostrando un suo utilizzo funzionale che possa rendere più consapevoli i ragazzi e le ragazze delle proprie abitudini online.
- Riflettere insieme su: come trascorri il tempo on line? Quando aggiunge valore alla tua vita e quando ti fa perdere tempo? Quale atteggiamento potresti cambiare quando sei online? Che ruolo ha e deve avere la tecnologia (internet o il gioco) nella tua vita?
- Proporre alle classi il questionario self/report sui fenomeni di bullismo e di cyberbullismo in forma anonima come ulteriore strumento di monitoraggio e segnalazione.
- Proporre delle alternative metodologiche e didattiche valide che abbiano come strumento giochi virtuali d'aula.
- Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/le studenti/studentesse.
- Generazioni Connesse ha realizzato un percorso con video interattivi per i/le ragazzi/e della scuola secondaria di primo grado (II e III classi) per affrontare il delicato tema del sexting (es. Susy - Ep. 5 Web-serie "Se Mi Posti Ti Cancello") e per affrontare il delicato tema dell'adescamento online (es. Laura - Ep. 4 Web-serie "Se Mi Posti Ti Cancello").
- Tenere sempre aperto un canale di comunicazione con gli alunni sui temi dell'affettività e del digitale.
- Fondamentale è portare avanti un percorso di educazione digitale che comprenda lo sviluppo di capacità, quali: la protezione della propria privacy e la gestione dell'immagine e dell'identità online, la capacità di gestire adeguatamente le proprie relazioni online (a partire dalla consapevolezza della peculiarità del mezzo/schermo che permette a chiunque di potersi presentare molto diversamente da come realmente è). A tal scopo la scuola propone a tutti gli alunni delle classi prime il progetto interistituzionale "Patente di smartphone", che comprende un percorso formativo sui dati sensibili, sul cyberbullismo e sul sexting.
- Organizzare incontri di sensibilizzazione e di prevenzione con esperti esterni (forze dell'ordine, associazioni, sanitari) sui rischi online e sull'utilizzo sicuro e consapevole delle tecnologie digitali.
- 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 (es. Save the Children)
- Organizzare incontri per la promozione del rispetto della diversità: differenze di genere, orientamento e identità sessuale, cultura e provenienza, etc., con la partecipazione attiva degli/le studenti/studentesse.
- Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/le studenti/studentesse. La scuola

propone a tutti gli alunni delle classi terze incontri con gli esperti del consultorio.

- Pianificare e realizzare progetti di peer-education - sui temi della sicurezza online. La scuola organizza la partecipazione, per tutti gli alunni delle classi seconde, al progetto #sbullizziamoci, che prevede gli interventi peer to peer degli alunni del liceo, opportunamente formati.

Nella prevenzione e nel contrasto alle varie forme di abuso che possono verificarsi sulla piattaforma online e non solo, la Scuola attua ricorrenti forme di collaborazione:

- con le Forze dell'ordine: Polizia Municipale, Arma dei Carabinieri, Polizia Postale (incontri e conferenze rivolti a tutti gli attori del processo educativo);
- con le associazioni presenti sul territorio e non solo, attraverso la proposta di rappresentazioni (es. teatrali) e laboratori agli studenti e alle studentesse.

I campanelli di allarme

Gli alunni possono mostrare segni di tristezza, di ansia o di risentimento nei confronti di compagni e/o altri e riferire spontaneamente o su richiesta l'accaduto ai docenti. I fatti riferiti possono essere accaduti anche al di fuori della scuola.

Il confronto periodico con gli alunni sui rischi delle comunicazioni on-line, può consentire ai minori di riferire fatti, eventi personali o altrui che "allertano" l'insegnante. Una "prova" di quanto riferito può essere presente nella memoria degli strumenti tecnologici utilizzati: può essere mostrata spontaneamente dall'alunno, può essere presentata da un reclamo dei genitori, può essere notata dall'insegnante che si accorge dell'infrazione in corso.

I contenuti "pericolosi" comunicati/ricevuti, messi/scaricati in rete, ovvero le tracce che possono comprovare l'utilizzo incauto, scorretto o criminoso degli strumenti digitali utilizzati dai minori, possono essere i seguenti:

- *contenuti afferenti alla privacy*: foto personali, indirizzo di casa o numero di telefono, informazioni private proprie o di amici, foto o video pubblicati contro la propria volontà, ecc.;
- *contenuti afferenti all'aggressività o alla violenza*: messaggi minacciosi, commenti offensivi, pettegolezzi, informazioni false, foto o video imbarazzanti, virus, contenuti razzisti, immagini o video umilianti, che inneggiano al suicidio, insulti, videogiochi pensati per un pubblico adulto, ecc.;
- *contenuti afferenti alla sessualità*: messaggi molesti, conversazioni (testo o voce) che connotano una relazione intima e/o sessualizzata, foto o video personali con nudità o abbigliamento succinto, immagini pornografiche, foto e video in cui dei minori sono coinvolti o assistono ad attività sessuali (pedopornografia), ecc.

Gestione dei casi di "immaturità"

Può sembrare naturale all'alunno fornire i propri dati ai siti allestiti per attrarre l'attenzione dei minori, con giochi e animazioni, personaggi simpatici e divertenti che richiedono una procedura di registrazione. Curiosità, manifestazioni di reciproco interesse tra pari, idee e fantasie sulla sessualità sono espressione da una parte del progressivo sviluppo socio-affettivo dell'alunno e dall'altra dei molteplici messaggi espliciti che gli giungono quotidianamente attraverso i media, i

discorsi dei pari o degli adulti. I comportamenti cosiddetti “quasi aggressivi”, che spesso si verificano tra coetanei, le interazioni animate o i contrasti verbali, o la presa in giro “per gioco”, effettuata anche in rete, mettono alla prova la relazione con i compagni, la supremazia o la parità tra i soggetti implicati e l’alternanza e sperimentazione dei diversi ruoli. Il gruppo dei pari rappresenta anche il momento di conquista dell’autonomia dall’adulto e pertanto è luogo di “complicità” e di piccole “trasgressioni”, di scambi “confidenziali” condivisi fra gli amici nella rete o con il cellulare. Detti comportamenti, che finiscono per arrivare all’attenzione degli adulti, sono controllati e contenuti dai docenti attraverso i normali interventi educativi, di richiamo al rispetto delle regole di convivenza civile e democratica, di rispetto degli altri, per evitare che possano degenerare, diventare pericolosi per sé o offensivi e minacciosi per gli altri.

QUESTIONARIO SELF REPORT SU EVENTUALI FENOMENI DI BULLISMO

Florence Bullying Victimization Scales (FBVSs)

Qui di seguito troverai alcune domande che riguardano le prepotenze tra ragazzi. Le domande riguardano la tua vita a scuola NEGLI ULTIMI 2-3 MESI (dall’inizio della scuola fino ad oggi). Quando rispondi cerca di pensare a tutto questo periodo e non soltanto ad ora.

Diciamo che un ragazzo/a subisce prepotenze quando un altro ragazzo/a o un gruppo di ragazzi/e:

- ★ gli/le dicono cose cattive e spiacevoli
- ★ lo/la prendono in giro
- ★ lo/la chiamano con nomi offensivi
- ★ lo/la ignorano o escludono completamente dal loro gruppo ★ non lo/la coinvolgono di proposito
- ★ gli/le danno colpi, calci, spinte o lo/la minacciano
- ★ dicono bugie o mettono in giro storie sul suo conto
- ★ inviano bigliettini con offese e parolacce
- ★ nessuno gli/le rivolge mai la parola

.....e altre cose di questo genere.

Questi fatti possono accadere spesso, ed è difficile per chi subisce prepotenze riuscire a difendersi. Si tratta di prepotenze quando un ragazzo/a viene preso/a in giro ripetutamente e con cattiveria. Non si tratta di prepotenze quando due ragazzi/e, all’incirca della stessa forza, litigano tra loro o fanno la lotta.

Quante volte hai subito prepotenze

NEGLI ULTIMI 2-3 MESI?

Punteggio Indicatore

- | | |
|---|---------------------------|
| 1 | Mai |
| 2 | solo una volta o due |
| 3 | 2 - 3 volte al mese |
| 4 | una volta a settimana |
| 5 | diverse volte a settimana |

In che modo hai subito prepotenze NEGLI ULTIMI 2-3 MESI? Indica con che frequenza ti è accaduto, facendo una croce su una delle possibili risposte.

Descrizione del comportamento	Punteggio attribuito
1. Sono stato picchiato	1 - 2 - 3 - 4 - 5
2. Sono stato chiamato con brutti nomi	1 - 2 - 3 - 4 - 5
3. Sono stato preso in giro	1 - 2 - 3 - 4 - 5
4. Sono stato ignorato dai miei compagni	1 - 2 - 3 - 4 - 5
5. Sono stato escluso dalle attività	1 - 2 - 3 - 4 - 5
6. Sono stato preso a calci e pugni	1 - 2 - 3 - 4 - 5
7. Hanno messo in giro delle voci sul mio conto	1 - 2 - 3 - 4 - 5
8. Mi hanno rubato o danneggiato degli oggetti	1 - 2 - 3 - 4 - 5
9. Sono stato spinto e strattonato	1 - 2 - 3 - 4 - 5
10. Sono stato insultato	1 - 2 - 3 - 4 - 5

Hai mai preso parte ad episodi di prepotenza
verso altri ragazzi/e NEGLI ULTIMI 2-3 MESI?

Punteggio Indicatore	
1	Mai
2	solo una volta o due
3	2 - 3 volte al mese
4	una volta a settimana
5	diverse volte a settimana

In che modo hai fatto prepotenze NEGLI ULTIMI 2-3 MESI? Indica con che frequenza ti è accaduto, facendo una croce su una delle possibili risposte.

Descrizione del comportamento	Punteggio attribuito
1. Ho picchiato qualcuno	1 - 2 - 3 - 4 - 5
2. Ho chiamato qualcuno con brutti nomi	1 - 2 - 3 - 4 - 5
3. Ho preso in giro qualcuno	1 - 2 - 3 - 4 - 5

- | | |
|---|-------------------|
| 4.
Ho ignorato qualche mio compagno | 1 - 2 - 3 - 4 - 5 |
| 5.
Ho escluso altri dalle attività | 1 - 2 - 3 - 4 - 5 |
| 6.
Ho preso a calci e pugni qualcuno | 1 - 2 - 3 - 4 - 5 |
| 7.
Ho messo in giro delle voci sul conto di qualcuno | 1 - 2 - 3 - 4 - 5 |
| 8.
Ho rubato o danneggiato degli oggetti | 1 - 2 - 3 - 4 - 5 |
| 9.
Ho spinto e stratonato qualcuno | 1 - 2 - 3 - 4 - 5 |
| 10.
Ho insultato qualcuno | 1 - 2 - 3 - 4 - 5 |

QUESTIONARIO SELF REPORT SU EVENTUALI FENOMENI DI CYBER BULLISMO

Florence Cyberbullying Cybervictimization Scales (FCBCVSs) brief version revised

Qui di seguito troverai alcune domande che riguardano una nuova forma di bullismo: il cyberbullismo. Il cyberbullismo è un comportamento aggressivo e di prevaricazione, come il bullismo, messo in atto tramite uno strumento elettronico come il PC o lo Smartphone e la rete: social networks come Facebook, Instagram, Whatsapp, sms, blog, ecc.

Le domande riguardano la tua vita NEGLI ULTIMI 2-3 MESI (dall'inizio della scuola fino ad oggi). Quando rispondi cerca di pensare a tutto questo periodo e non soltanto ad ora.

1. Quante volte hai subito episodi di cyber bullismo NEGLI ULTIMI 2-3 MESI?

Punteggio Indicatore

- | | |
|---|---------------------------|
| 1 | Mai |
| 2 | solo una volta o due |
| 3 | 2 - 3 volte al mese |
| 4 | una volta a settimana |
| 5 | diverse volte a settimana |

NEGLI ULTIMI 2-3 MESI (DALL'INIZIO DELLA SCUOLA FINO AD OGGI) QUANTE VOLTE TI È CAPITATO DI...

Descrizione del comportamento	Punteggio attribuito
1. Di ricevere minacce e insulti su internet (Social networks, chat, blog etc.)	1 - 2 - 3 - 4 - 5
2. Di essere escluso o lasciato fuori da gruppi on-line (Social networks, chat, blog etc.)	1 - 2 - 3 - 4 - 5
3. Di trovare o ricevere foto o video imbarazzanti o intime che ti riguardano (su Social networks, chat, blog etc.)	1 - 2 - 3 - 4 - 5
4. Che qualcuno si sia impadronito di informazioni o materiale personale (es. password, foto etc.) per poi riutilizzarli	1 - 2 - 3 - 4 - 5

Hai mai preso parte ad episodi di cyber bullismo verso altri ragazzi/e NEGLI ULTIMI 2/3 MESI?

Punteggio Indicatore

- | | |
|---|---------------------------|
| 1 | Mai |
| 2 | solo una volta o due |
| 3 | 2 - 3 volte al mese |
| 4 | una volta a settimana |
| 5 | diverse volte a settimana |

4.2 - Quali strumenti e a chi

L'insegnante riveste la qualifica di pubblico ufficiale (ex [art. 357 c.p.](#)) 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.

Il Codice Penale Italiano, all'[art. 357](#), definisce il pubblico ufficiale come colui che esercita una "pubblica funzione legislativa, giudiziaria o amministrativa". Questa definizione si estende ai docenti nel momento in cui sono impegnati nell'esercizio delle loro funzioni all'interno degli istituti scolastici.

La Corte di Cassazione, con la sentenza [n. 15367/2014](#), ha ribadito la qualifica di pubblico ufficiale per l'insegnante, estendendo tale riconoscimento non solo alla tenuta delle lezioni, ma anche a tutte le attività connesse. Questo include, ad esempio, gli incontri con i genitori degli allievi.

Le situazioni problematiche in relazione all'uso delle tecnologie digitali dovrebbero essere sempre gestite da un team di docenti composto da:

1. Dirigente
2. Docente referente,
3. L'animatore digitale (secondo il Piano Nazionale per la Scuola Digitale, abbreviato in PNSD, introdotto dalla Legge 107/2015)
4. Referente bullismo (ex. Legge Italiana Contro il Cyberbullismo, l. 71/2017)
5. Altri docenti già impegnati nelle attività di promozione dell'educazione civica.

Le situazioni di pregiudizio presunto o reale possono richiedere il supporto e l'intervento di esperti esterni alla scuola.

Come descritto nelle procedure di questa sezione, si potrebbero palesare due macro - 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.

In questo caso, l'informazione relativa al sospetto deve essere inoltrata al Referente e al team dei docenti "antibullismo" con l'obiettivo di allertare il Dirigente. La comunicazione dovrebbe avere una forma scritta e riportare tutti i dati e le

informazioni in maniera dettagliata e oggettiva. Da qui, il Dirigente e i docenti coinvolti procedono alla valutazione del caso (valutare l'invio o meno della relazione agli organi giudiziari preposti) e agiscono tramite percorsi di sensibilizzazione.

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.

In questo caso, l'informazione relativa al sospetto deve essere inoltrata al Referente e al team dei docenti "antibullismo" con l'obiettivo di allertare il Dirigente. La comunicazione dovrebbe avere una forma scritta e riportare tutti i dati e le informazioni in maniera dettagliata e oggettiva. Da qui, si procede alla valutazione approfondita e alla verifica di quanto segnalato, avviando (se appurato la rilevanza penale) la procedura giudiziaria con denuncia all'autorità giudiziaria per attivare un procedimento penale.

Qualora si rilevasse un fatto riconducibile alla fattispecie di reato, l'insegnante - nel ruolo di pubblico ufficiale - non deve procedere con indagini di accertamento ma ha sempre l'obbligo di segnalare l'evento all'autorità giudiziaria. (ex. l. 71/2017). Con autorità competente si intendono:

- Procure Ordinarie: nel caso in cui il minore/i sia la vittima/e e il presunto autore del reato sia maggiorenne,
- Procura Minorile: in caso il presunto autore del reato sia minorenni.

Vi è anche l'obbligatorietà della segnalazione delle situazioni di pregiudizio a carico dei minori: L. 216/1991: per le situazioni di grave rischio l'istituzione scolastica è tenuta alla segnalazione delle medesime. Per pregiudizio si intende una condizione di rischio o grave difficoltà che provocano un danno reale o potenziale alla salute, alla sopravvivenza, allo sviluppo o alla dignità del bambino, nell'ambito di una relazione di responsabilità, fiducia o potere.

La segnalazione come da procedura interna è il primo passo per aiutare un minore che vive una situazione di rischio o di grave difficoltà e va intesa come un momento di condivisione e solidarietà nei confronti del minore. La mancata segnalazione costituisce, infatti, omissione di atti d'ufficio (art.328 C.P.).

Può essere utile, valutando accuratamente ciascuna situazione, attivare colloqui individuali con tutti i minori coinvolti, siano essi vittime, testimoni e/o autori. È importante considerare il possibile coinvolgimento dei genitori e di coloro incaricati della tutela dei minori coinvolti. L'intervento va indirizzato valutando l'eventuale impatto educativo e/o il contesto emotivo senza discriminare tra vittime, testimoni e/o autori.

Prevedere possibili incontri di mediazione tra i minori coinvolti vanno ponderati con la consapevolezza del loro stato emotivo, anche e in base agli elementi raccolti in merito del fatto/episodio avvenuto (elementi che si dovrebbero valutare di caso in caso). Importante è prevedere il coinvolgimento dei genitori sia della vittima che del bullo (ove possibile).

Anche i genitori devono e possono segnalare casi di sospetto o evidenza dei fenomeni, segnalarlo al Dirigente, o al docente coordinatore di classe o referente di istituto oppure direttamente al team antibullismo attraverso apposita procedura che definisce l'istituto (mail ad hoc, tramite gli uffici e postazioni specifiche, etc...).

Gli insegnanti e i genitori, come studenti e studentesse, si possono rivolgere alla Helpline del progetto Generazioni Connesse, al numero gratuito 19696, attraverso la chat disponibile sul [sito](#) o tramite chat WhatsApp per ricevere supporto e consulenza. Per tutti i dettagli, il riferimento è agli allegati con le procedure.

Strumenti a disposizione di studenti/esse

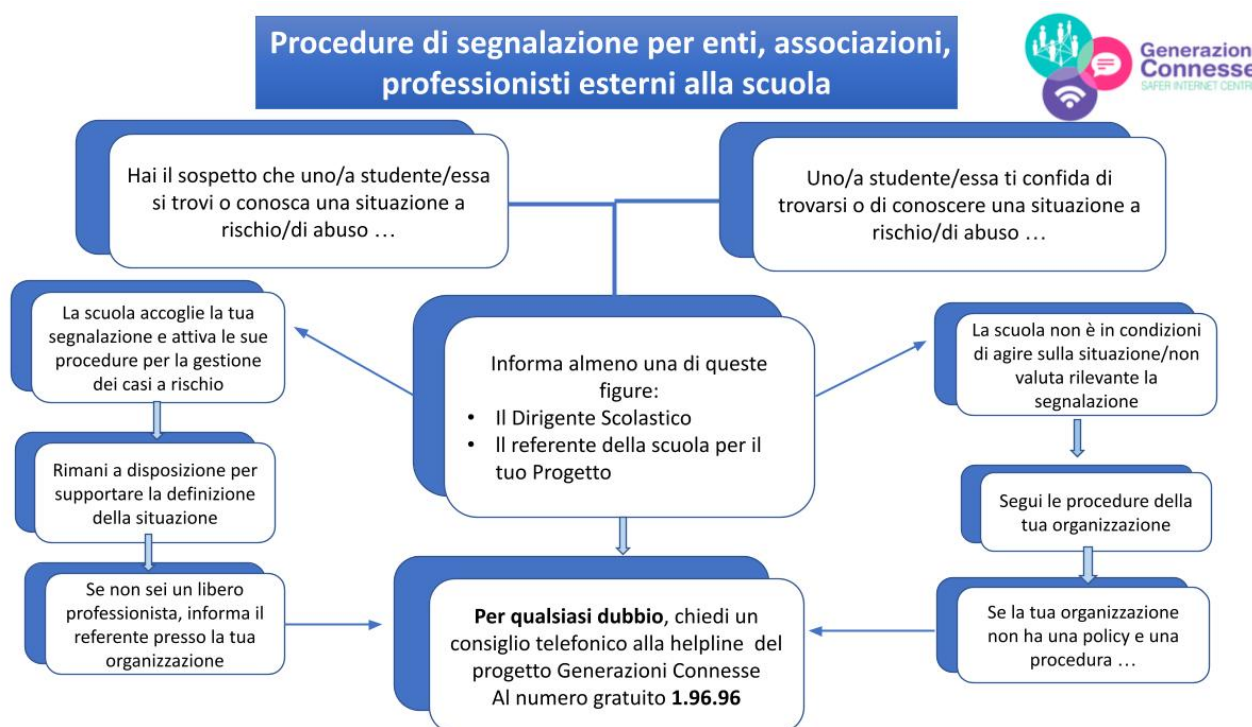
Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione: un indirizzo e-mail specifico per le segnalazioni; scatola/box per la raccolta di segnalazioni anonime da inserire in uno spazio accessibile e ben

visibile della scuola; sportello di ascolto con professionisti; docente referente per le segnalazioni.

In particolare, sarebbe utile che la scuola attivi un sistema di segnalazione utile anche al monitoraggio dei fenomeni dal quale partire per integrare azioni didattiche preventive e giornate di sensibilizzazione, insieme agli Enti/Servizi presenti sul territorio di riferimento. Importante, altresì, immaginare e programmare percorsi di peer education per la prevenzione e il contrasto degli agiti.

Per ulteriori chiarimenti in merito, si rimanda al Regolamento di disciplina degli studenti e delle studentesse, integrato con la previsione di infrazioni disciplinari legate a comportamenti scorretti assunti durante la DID e relative sanzioni, alle [Linee di Orientamento per la prevenzione e il contrasto dei fenomeni di Bullismo e Cyberbullismo del MI \(Ministero dell'Istruzione\)](#) aggiornate al 2021, al Patto educativo di corresponsabilità e annessa appendice relativa agli impegni che le parti in causa dovranno assumere per l'espletamento efficace della DID e, in ultimo, al Piano scolastico per la Didattica Digitale Integrata, allegato al PTOF.

Procedure



Procedure interne: cosa fare in caso di evidenza di Cyberbullismo



Il docente ha evidenza che stia accadendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo

Se non è già stato fatto, avvisa il referente per il cyberbullismo (e/o il team antibullismo) che attiva le procedure ("Corso 4" della piattaforma ELISA) e il Dirigente Scolastico.

Ricordare sempre che in base alla legge 71-2017:

A) Se c'è fattispecie di reato va fatta la segnalazione alle forze dell'ordine

B) Se non c'è fattispecie di reato.

Il DS (e/o il team antibullismo):

- informa i genitori (o chi esercita la responsabilità genitoriale) dei ragazzi/e direttamente coinvolti (qualsiasi ruolo abbiano avuto) su quanto accade e condivide informazioni e strategie.
- Informa i genitori di ragazzi/e 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)
- Attiva il consiglio di classe.

Se, come docente, hai un dubbio su come procedere o interpretare quello che sta accadendo, puoi chiedere in qualsiasi momento, una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

NELLE CLASSI

Il team antibullismo collabora coi docenti della classe per realizzare l'intervento nella classe:

a seconda della situazione valutata se

- affrontare direttamente l'accaduto o
- sensibilizzare la classe (vedi Corso 4 Piattaforma Elisa)
- trova il modo di supportare la vittima e di responsabilizzare i compagni rispetto al loro ruolo, anche di spettatori, nella situazione.

A seconda della situazione e delle valutazioni operate con referente, dirigente e genitori, segnala alla Polizia Postale:

a) contenuto; b) modalità di diffusione.

Se è opportuno, richiedi un sostegno ai servizi territoriali o ad altre Autorità competenti (soprattutto se il cyberbullismo non si limita alla scuola).

Procedure interne: cosa fare in caso di sospetto di Cyberbullismo



Il docente riceve una segnalazione (da un genitore, un altro studente ...) o sospetta che stia accadendo qualcosa a uno/a studente/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo

Ricorda agli studenti che possono segnalare al gestore del sito/social e al garante privacy eventuali contenuti offensivi/lesivi che li riguardano

Condividi con il referente o al team antibullismo: si attiva il processo di attenzione e valutazione a cura del referente.

Insieme si valuta se è il caso

- di avvisare il consiglio di classe;
- di avvisare il Dirigente Scolastico, anche in base al regolamento interno o a prassi consolidate.

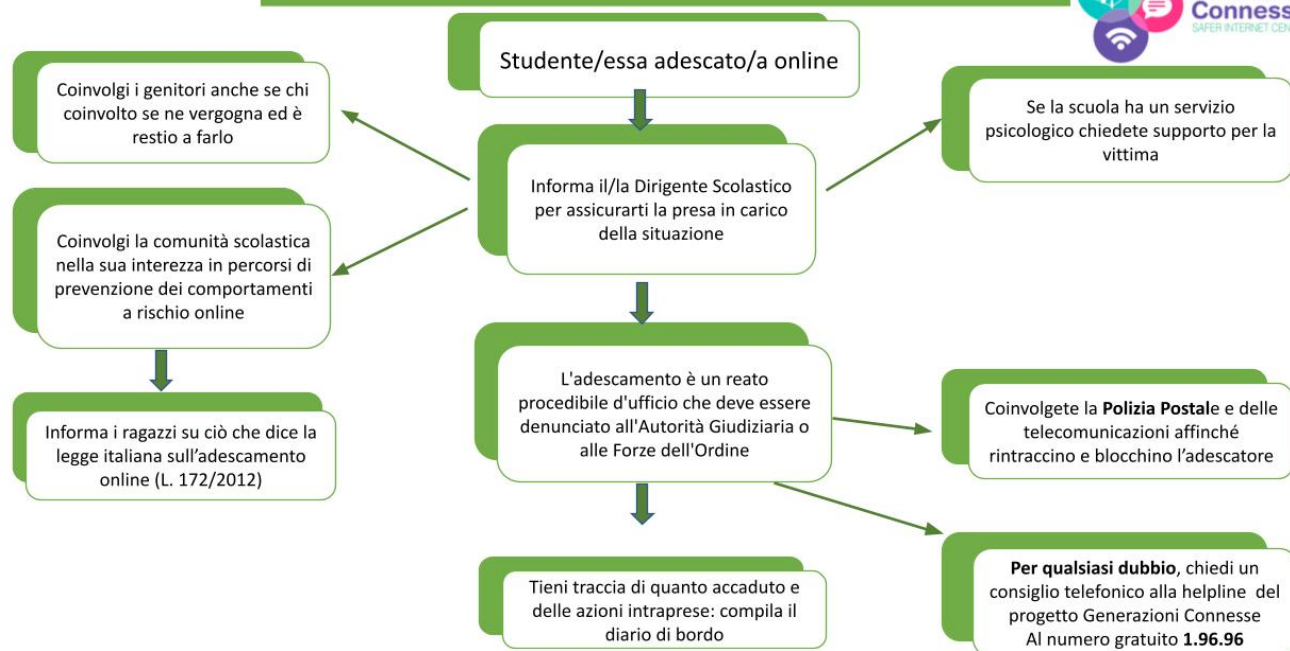
Se, come docente, hai un dubbio su come procedere o interpretare quello che sta accadendo, puoi chiedere in qualsiasi momento, una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

Scarica le linee di orientamento per la prevenzione e il contrasto dei fenomeni di bullismo e cyberbullismo

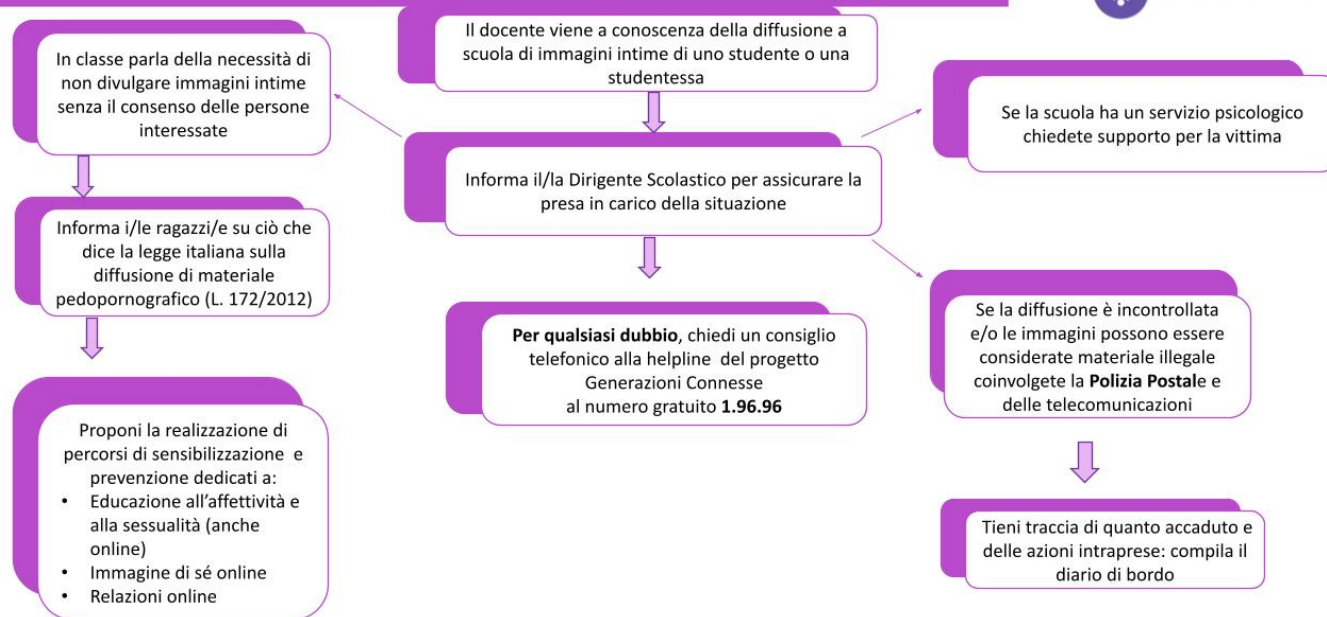
Se emergono evidenze passa allo schema successivo

Ricorda a studenti/esse che possono chiedere in qualsiasi momento una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96 o via chat

Procedure interne: cosa fare in caso di Adescamento Online?



Procedure interne: cosa fare in caso di diffusione non consensuale di immagini intime?



Procedura di intervento relativa ai fenomeni di prepotenza

Il docente che assiste al fenomeno, o che accoglie nell'immediato il racconto, sente le parti in causa, avvia:

- la segnalazione alle famiglie con annotazione sul diario, nel caso in cui le condizioni siano tali da non permettere una pacificazione tra le parti;
- la compilazione della scheda di segnalazione che invia al referente del bullismo e del cyberbullismo per informare e ricevere eventuali successivi contributi.

IN SITUAZIONI DI EMERGENZA:

qualora il docente si trovasse in difficoltà nel gestire la situazione, si rivolgerà al TEAM DI EMERGENZA tramite il servizio di segreteria, che metterà il docente in contatto con (di seguito in ordine di precedenza, considerata la presenza in loco):

1. Dirigente scolastico
2. Vicario
3. Referente bullismo/cyberbullismo
4. Animatore digitale
5. Referente continuità
6. Referente progetto Stra-ordinario
7. Docente di strumento indirizzo musicale

Raccomandazioni relative a fenomeni di cyberbullismo:

- Assicurarsi che l'alunno/a vittima salvi nel suo telefono ogni messaggio, voce/testo/immagine, conservando così il numero del mittente.
- I docenti, anche con l'ausilio tecnico dell'Animatore digitale, possono provvedere ugualmente a conservare le prove della condotta incauta, scorretta o dell'abuso rilevati sui pc della scuola: soprattutto la data e l'ora, il contenuto dei messaggi, e, se possibile, l'ID del mittente (es. username, mail, numero di telefono cellulare) o l'indirizzo web del profilo e il suo contenuto.
- Per gli eventuali collegamenti non autorizzati a siti social network, video-hosting sites e altri website, l'insegnante può conservare il link, stampare la pagina o salvare la schermata su documento word. Per le e-mail si può stampare la mail o conservare l'intero messaggio, compresa l'intestazione del mittente.
- Conservare la prova è utile per far conoscere l'accaduto in base alla gravità ai genitori degli alunni, al Dirigente

scolastico e, per le condotte criminose, alla polizia.

- Qualora non si disponga di prove ma solo delle testimonianze dell'alunno, quantunque riferite a fatti accaduti al di fuori del contesto scolastico, le notizie raccolte sono comunque comunicate ai genitori e per fatti rilevanti anche al Dirigente scolastico; per quelle criminose, anche alla polizia.
- La segnalazione viene fatta ad entrambe le famiglie, se oltre alla vittima anche l'autore della condotta negativa è un altro alunno.
- Per i reati meno gravi la legge rimette ai genitori degli alunni la scelta di richiedere la punizione del colpevole, attraverso la querela.
- Per i reati più gravi (es. pedopornografia) gli operatori scolastici hanno l'obbligo di effettuare la denuncia all'autorità giudiziaria (o più semplicemente agli organi di polizia territorialmente competenti). In particolare, per i fatti criminosi, ai fini della denuncia, la relazione deve essere circostanziata, cioè redatta nel modo più accurato possibile, indicando i seguenti elementi: il fatto, il giorno dell'acquisizione del fatto nonché le fonti di prova già note e, per quanto possibile, le generalità, il domicilio e quant'altro di utile a identificare la persona alla quale il reato è attribuito, la persona offesa e tutti coloro che sono in grado di riferire circostanze rilevanti per la ricostruzione del fatto.

Procedure operative per la rilevazione, il monitoraggio e la gestione delle segnalazioni.

A chi segnalare:

- l'attuazione del programma di intervento si basa prevalentemente sull'impiego delle risorse umane già presenti e disponibili: il referente al cyberbullismo, tutti i docenti e il personale scolastico, gli alunni e i genitori, il servizio dello sportello di ascolto. Non serve, se non in casi particolarmente gravi, l'opera di psicologi, assistenti sociali o altri specialisti a cui orientare la famiglia. L'elemento fondamentale per una buona riuscita del programma è infatti la corretta ristrutturazione del contesto relazionale degli alunni.
- nel caso in cui ci si dovesse imbattere in materiale pedopornografico (cioè contenuti foto e video in cui persone di minore età sono coinvolte o assistono ad attività sessuali), è necessario, innanzitutto, evitare di eseguire download, produrne copie, condividerne link o postarne il contenuto. Ciò è reato per chiunque. Nel venire a conoscenza di materiali di questo tipo è importante contribuire alla loro eliminazione: basta inserire le informazioni richieste sugli appositi moduli online, disponibili ai siti www.stopit.it e <http://www.azzurro.it/it/clicca-e-segnala> ovvero collegandosi al sito della polizia postale <https://www.commissariatodips.it>, ove è possibile sia segnalare che denunciare. In alternativa è possibile recarsi nella sede più vicina della polizia giudiziaria. Ciò consente di operare con la massima tempestività. È bene non operare in modo isolato, ma confrontarsi con i colleghi di classe e il Dirigente Scolastico.

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.

MODULO PER LA SEGNALEZIONE DI PRESUNTI CASI DI BULLISMO E/O CYBERBULLISMO

Nome di chi compila la segnalazione..... Ruolo.....

Data.....

Descrizione dell'episodio o del problema	Vittima/e:	Classe:
Soggetti coinvolti	Bullo/i:	Classe:
Chi ha riferito dell'episodio?	☐ La vittima..... ☐ Un compagno della vittima, nome: ☐ Genitore, nome: ☐ Insegnante, nome: ☐ Altri, specificare:	

Da quanti compagni è sostenuto il bullo?

Atteggiamento del gruppo Quanti compagni supportano la vittima o potrebbero farlo?

Gli insegnanti sono intervenuti?

Se sì, in che modo?

La famiglia o altri adulti hanno cercato di intervenire?

Se sì, in che modo?

Chi è stato informato della situazione?

☐ coordinatore di classe.....data:

☐ consiglio di classe data:

☐ dirigente scolastico data:

☐ la famiglia della vittima/e..... data:

☐ la famiglia del bullo/i data:

☐ le forze dell'ordine data:

☐ altro, specificare: